

3 1761 11972098 5



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761119720985>

83
97
HOUSE OF COMMONS

Issue No. 1

Thursday, March 10, 1983
Tuesday, March 15, 1983
Thursday, March 17, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 1

Le jeudi 10 mars 1983
Le mardi 15 mars 1983
Le jeudi 17 mars 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Organization meeting

Order of Reference: Study to examine the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime

Matters pertaining to the Order of Reference

CONCERNANT:

Séance d'organisation

Ordre de renvoi: Étude pour étudier l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs

Questions relatives à l'Ordre de renvoi

WITNESSES:

(See back cover)



TÉMOINS:

(Voir à l'endos)

First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Ray Hnatyshyn
Claude-André Lachance
Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS DÉSI-
GNÉS

Perrin Beatty
W. Kenneth Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee



STANDING COMMITTEE ON JUSTICE AND LEGAL
AFFAIRS

ORDER OF REFERENCE

Tuesday, March 1, 1983

ORDERED,—That a Sub-committee of the Standing Committee on Justice and Legal Affairs be formed to examine the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, and that the Sub-committee be composed of four members representing the three parties, that the members be chosen by the Chairman, after the usual consultations with the Whips of the different parties;

That the said Sub-committee be empowered to send for persons, papers and records, to sit while the House is sitting, to sit during periods when the House stands adjourned, to print from day to day such papers and evidence as may be ordered by it, and that the Chairman of the Sub-committee be authorized to hold meetings, to receive and authorize the printing of evidence when a quorum is not present; and

That the said Sub-committee report to this Committee no later than March 31, 1983.

*ATTEST*COMITÉ PERMANENT DE LA JUSTICE ET DES
QUESTIONS JURIDIQUES

ORDRE DE RENVOI

Le mardi 1^{er} mars 1983

IL EST ORDONNÉ,—Qu'un Sous-comité du Comité permanent de la justice et des questions juridiques soit constitué pour étudier l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs, et que ce Sous-comité soit composé de quatre membres représentant les trois partis, que ces membres soient désignés par le président, après les consultations d'usage avec les whips des différents partis;

Que le ledit Sous-comité soit autorisé à convoquer des personnes et à exiger la production de documents et dossiers, à se réunir pendant que la Chambre siège et pendant les périodes où la Chambre est ajournée, à faire imprimer au jour le jour les documents et témoignages dont il peut ordonner l'impression et à autoriser le président du Sous-comité à tenir des réunions pour entendre les témoignages et en autoriser la publication en l'absence d'un quorum; et

Que le dit Sous-comité fasse rapport au Comité au plus tard le 31 mars 1983.

*ATTESTÉ**Le greffier du Comité permanent de la justice et des questions juridiques*

Bernard G. Fournier

Clerk of the Standing Committee on Justice and Legal Affairs

MINUTES OF PROCEEDINGS

THURSDAY, MARCH 10, 1983

(1)

[Text]

The Sub-committee on Computer Crime met this day at 5:34 o'clock p.m. for the purpose of organization.

Members of the Sub-committee present: Mrs. Hervieux-Payette, Messrs. Hnatyshyn and Lachance.

Designated Alternate Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

Other Member present: Mr. MacBain.

In attendance: Mr. P. Rosen and Mrs. M. Hébert, Researchers, Research Branch, Library of Parliament.

The Clerk presided over the election of the Chairman of the Sub-committee.

Mr. Lachance moved,—That Mrs. Céline Hervieux-Payette do take the Chair of this Sub-committee as Chairman.

The question being put on the motion, it was agreed to.

The Chairman took the Chair.

On motion of Mr. Lachance, it was agreed,—That the Chairman be authorized to hold meetings, to receive and authorize the printing of evidence when a quorum is not present.

On motion of Mr. Lachance, it was agreed,—That the Sub-committee have 1,000 copies of their Minutes of Proceedings and Evidence printed.

On motion of Mr. Lachance, it was agreed,—That the Sub-committee be named Sub-committee on Computer Crime of the Standing Committee on Justice and Legal Affairs.

On motion of Mr. Lachance, it was agreed,—That the Chairman be authorized to arrange meetings and to make the necessary arrangements to have witnesses appear before the Sub-committee after consultation with other members of the Sub-committee.

Mr. Lachance moved,—That, when requested by the witness, reasonable travelling and living expenses be paid to witnesses who are invited to appear before the Sub-committee in relation to its Order of Reference.

After debate, the question being put on the motion, it was agreed to.

On motion of Mr. Lachance, it was agreed,—That the Sub-committee meet on Tuesday, March 15, 1983 at 5:00 o'clock p.m. in order to plan its future business.

At 5:49 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

TUESDAY, MARCH 15, 1983

(2)

The Sub-committee on Computer Crime met this day at 5:12 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

PROCÈS-VERBAL

LE JEUDI 10 MARS 1983

(1)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs tient aujourd'hui à 17h34 sa séance d'organisation.

Membres du Sous-comité présents: M^{me} Hervieux-Payette, MM. Hnatyshyn et Lachance.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Autre député présent: M. MacBain.

Aussi présents: M. P. Rosen et M^{me} M. Hébert, recherchistes du Service de la recherche de la Bibliothèque du Parlement.

Le greffier préside à l'élection du président du Sous-comité.

M. Lachance propose,—Que M^{me} Céline Hervieux-Payette soit nommée président du Sous-comité.

La motion, mise aux voix, est adoptée.

La présidente prend place au fauteuil.

Sur motion de M. Lachance, il est convenu,—Que le président soit autorisé à tenir des séances pour recevoir des témoignages et en autoriser l'impression, en l'absence d'un quorum.

Sur motion de M. Lachance, il est convenu,—Que le Sous-comité fasse imprimer 1,000 exemplaires de ses procès-verbaux et témoignages.

Sur motion de M. Lachance, il est convenu,—Que le Sous-comité porte le nom de Sous-comité sur les infractions relatives aux ordinateurs du Comité permanent de la justice et des questions juridiques.

Sur motion de M. Lachance, il est convenu,—Que le président soit autorisé à prévoir des séances et prendre des dispositions pour la comparution des témoins après consultation avec les autres membres du Sous-comité.

M. Lachance propose,—Que lorsqu'un témoin en fait la demande, des frais raisonnables de déplacements et de séjour soient versés aux témoins invités à comparaître devant le Sous-comité concernant son Ordre de renvoi.

Après débat, la motion, mise aux voix, est adoptée.

Sur motion de M. Lachance, il est convenu,—Que le Sous-comité se réunisse le mardi 15 mars 1983 à 17h00 afin de planifier ses travaux futurs.

A 17h49, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

LE MARDI 15 MARS 1983

(2)

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 17h12, sous la présidence de M^{me} Céline Hervieux-Payette, Président.

Designated Alternate Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee proceeded to consider its Order of Reference dated Tuesday, March 1, 1983 which reads as follows:

ORDERED—That a Sub-committee of the Standing Committee on Justice and Legal Affairs be formed to examine the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, and that the Sub-committee be composed of four members representing the three parties, that the members be chosen by the Chairman, after the usual consultations with the Whips of the different parties;

—That the said Sub-committee be empowered to send for persons, papers and records, to sit while the House is sitting, to sit during periods when the House stands adjourned, to print from day to day such papers and evidence as may be ordered by it, and that the Chairman of the Sub-committee be authorized to hold meetings, to receive and authorize the printing of evidence when a quorum is not present; and

—That the said Sub-committee report to this Committee no later than March 31, 1983.

It was agreed,—That Senior Officials from the Department of Justice be invited to appear before the Sub-committee in relation with its Order of Reference, on Thursday, March 17, 1983, at 3:30 o'clock p.m.

At 5:21 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

THURSDAY, MARCH 17, 1983

(3)

The Sub-committee on Computer Crime met this day at 3:12 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From the Department of Justice: Mr. Norman Hill, Project Chief, Theft and Fraud Project, and Mr. Neville Avison, Chief, Research and Statistics. *From the Royal Canadian Mounted Police:* Superintendent George W. Allen, Commercial Crime Branch.

The Sub-Committee resumed consideration of its Order of Reference, dated, Tuesday, March 1st, 1983. (*See Minutes of Proceedings of Tuesday, March 15, 1983.*)

Mr. Hill and Mr. Allen made a statement and, with the other witness, answered questions.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de recherche, Bibliothèque du Parlement.

Le Sous-comité entreprend l'étude de son Ordre de renvoi du mardi, 1^{er} mars 1983, qui se lit comme suit:

IL EST ORDONNÉ,—Qu'un Sous-comité du Comité permanent de la justice et des questions juridiques soit constitué pour étudier l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs, et que ce Sous-comité soit composé de quatre membres représentant les trois partis, que ces membres soient désignés par le président, après les consultations d'usage avec les whips des différents partis;

—Que ledit Sous-comité soit autorisé à convoquer des personnes et à exiger la production de documents et dossiers, à se réunir pendant que la Chambre siège et pendant les périodes où la Chambre est ajournée, à faire imprimer au jour le jour les documents et témoignages dont il peut ordonner l'impression et à autoriser le président du Sous-comité à tenir des réunions pour entendre les témoignages et en autoriser la publication en l'absence d'un quorum; et

—Que ledit Sous-comité fasse rapport au Comité au plus tard le 31 mars 1983.

Il est convenu,—Que des haut-fonctionnaires du Ministère de la justice soient invités à comparaître devant le Sous-comité au sujet des questions relatives à son Ordre de renvoi, le jeudi 17 mars 1983 à 15h30.

A 17h21, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

LE JEUDI 17 MARS 1983

(3)

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h12, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: Du ministère de la Justice: M. Norman Hill, Chef de projet, Projet vol et fraude et M. Neville Avison, Chef, Recherche et statistiques. *De la Gendarmerie royale du Canada:* Surintendant George W. Allen, Section délits commerciaux.

Le Sous-comité reprend l'étude de son Ordre de renvoi, du mardi, 1^{er} mars 1983. (*Voir procès-verbaux du mardi 15 mars 1983.*)

MM. Hill et Allen font une déclaration et, avec l'autre témoin, répondent aux questions.

At 5:21 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

A 17h21, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-Committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Thursday, March 10, 1983

• 1732

The Clerk of the Committee: I see that we now have a quorum. The first item on today's agenda is the election of a chairman. I am now ready to receive any motion to that effect. Mr. Lachance.

Mr. Lachance: It will probably be the first and last time you will see me in this subcommittee because of the technicality that I just explained to the members, but since I am here, I am very glad to propose Madam Céline Hervieux-Payette as chairperson of the subcommittee.

Mr. Robinson (Etobicoke—Lakeshore): I second the motion.

Motion agreed to.

Le greffier: J'inviterais M^{me} Hervieux-Payette à venir occuper le fauteuil, s'il vous plaît.

Le président: Nous allons maintenant procéder à l'élection d'un vice-président ou d'une vice-présidente. Est-ce qu'il y a quelqu'un qui...

Mr. Lachance: You have a problem. I do not think you can elect, officially, a vice-chairman, except maybe Ms McDonald or Mr. Beatty. I do not know how it works, about the problem of permanent members as opposed to alternate members. I know you and Mr. Beatty could not, because an alternate, so what I would suggest is that you elect yourself an unofficial chairperson for the purpose of the subcommittee, or unless otherwise advised by the clerks. You might have a problem, legally speaking, if you do. But unofficially you can do it. There is no problem whatsoever. An acting vice-chairperson, if you want.

• 1735

The Chairman: We will wait until we have our next subcommittee meeting since the full membership will be there.

Mr. Hnatyshyn: You will not have any voting members there except yourself.

The Chairman: Well, if Lynn is attending... She will not?

Mr. Hnatyshyn: I cannot speak for her, but I would be very surprised if you see her.

Mr. Lachance: You have here the core of your membership: Mr. Beatty, Mr. Robinson and yourself. Miss McDonald has advised us because of the restrictions of their caucus that... She is the ordinary NDP member, but I do not think she will participate very much in your work.

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le jeudi 10 mars 1983

Le greffier du Comité: Je remarque que nous avons le quorum. Nous allons donc passer au premier article à l'ordre du jour, soit l'élection d'un président. Je suis prêt à entendre des motions à cette fin. Monsieur Lachance.

M. Lachance: C'est probablement la première et dernière fois que j'assisterai à une réunion de ce Sous-comité, et ce pour des raisons techniques que je vais expliquer aux membres. Toutefois, étant donné que je suis ici, il me fait plaisir de proposer l'élection de M^{me} Céline Hervieux-Payette à la présidence du Sous-comité.

M. Robinson (Etobicoke—Lakeshore): J'appuie cette proposition.

La motion est adoptée.

The Clerk: I now invite Mrs. Hervieux-Payette to please come to the chair.

The Chairman: We will now proceed with the election of a vice-chairman. Does anyone want to...

M. Lachance: Vous faites face à un problème ici, car je ne crois pas qu'il vous soit possible d'élire officiellement un vice-président, sauf s'il s'agit de M^{me} McDonald ou de M. Beatty. J'ignore comment fonctionne le système eu égard à la question des membres permanents par opposition aux membres substitués. Je sais cependant que vous et M. Beatty ne pouvez pas procéder à l'élection puisque vous êtes membres substitués; je vous proposerai donc de vous élire un vice-président non officiel, à moins que les greffiers ne vous conseillent de faire autre chose. Autrement, vous aurez peut-être des problèmes sur le plan juridique, que vous n'aurez pas si vous le faites à titre non officiel. Il s'agirait alors d'un vice-président intérimaire, si vous voulez.

Le président: Nous allons attendre la prochaine réunion du Comité étant donné que tous ses membres y seront présents.

M. Hnatyshyn: Cependant, aucun des membres n'aura le droit de vote sauf vous-même.

Le président: Eh bien, si Lynn est présente, est-ce qu'elle n'aura pas le droit de vote?

M. Hnatyshyn: Je ne puis parler en son nom, mais je serais très étonnée qu'on la voit.

M. Lachance: Les principaux membres du Sous-comité sont ici: M. Beatty, M. Robinson et vous-même. Quant à M^{lle} McDonald, elle nous a laissé savoir qu'étant donné les restrictions imposées à son caucus... Elle est le membre régulier représentant le NPD, mais je crois pas qu'elle participera beaucoup à vos travaux.

[Text]

Mr. Hnatyshyn: She will certainly keep informed as to what is happening and appear if and when necessary, but I would not count on her as a . . .

Mr. Lachance: Maybe the subcommittee could consult with its own members and maybe it could decide to have one of its numbers as an unofficial vice-chairperson to be able to have meetings when Mrs. Hervieux-Payette is not there.

The Chairman: I would really have to be sick.

Mr. Lachance: Maybe you could put now the motions you have to put for printing and that kind of thing so that we can deal with other things.

The Chairman: Yes, that is what I am going to do.

Alors, maintenant il faut une motion pour proposer que le président puisse recevoir les témoignages et en autoriser l'impression lorsqu'il y a absence de quorum. Est-ce qu'il y a un proposeur?

M. Lachance: Oui.

Le président: La motion est proposée par M. Lachance. Est-ce que tout le monde est d'accord?

La motion est adoptée

Le président: Maintenant il faut une motion pour proposer l'impression des fascicules des procès-verbaux et des témoignages . . . Doit-on donner le nombre de copies?

Une voix: Mille copies.

Le président: Mille copies?

Mr. Lachance: Do you think you need 1,000? What do you think? What is the demand?

The Chairman: That is the minimum. We wanted to have the minimum before we started counting and we arrived at 1,000 whether we like it or not.

Mr. Lachance: Okay, fine for 1,000.

La proposition est adoptée.

Le président: Une proposition pour donner un titre . . . a name to the subcommittee.

I have a suggestion that the committee be named the Subcommittee on Computer Crime of the Standing Committee of Justice and Legal Affairs.

Some hon. Members: Agreed.

Mr. Robinson (Etobicoke—Lakeshore): What is the . . . Question.

The Chairman: Subcommittee on Computer Crime.

Mr. Robinson (Etobicoke—Lakeshore): No, no. A question of the chairman: what are the terms of reference of the committee? Is this from the terms of reference?

Mr. Lachance: The subject-matter of Mr. Beatty's bill.

Mr. Beatty: Which is computer crime.

[Translation]

M. Hnatyshyn: Elle va certainement nous tenir au courant de ce qui se passe, et être présente lorsque cela sera nécessaire, mais je ne compterais pas sur elle comme . . .

M. Lachance: Le Comité pourrait peut-être consulter ses membres afin qu'on nomme peut-être un vice-président non officiel, ce qui permettrait la tenue de réunions, en l'absence de M^{me} Hervieux-Payette.

Le président: Il faudra que je sois vraiment malade.

M. Lachance: Maintenant, vous pourriez peut-être entendre les motions relatives à l'impression, etc., afin que nous puissions passer à autre chose.

Le président: Oui, c'est ce que je vais faire.

We now need a motion enabling the chairman to hear witnesses and have the minutes printed when there is no quorum. Is there a mover?

Mr. Lachance: Yes.

The Chairman: The motion is put forward by Mr. Lachance. Does everyone agree?

The motion is carried.

The Chairman: Now we need a motion for the purpose of printing the Minutes of Proceedings . . . must we specify the number of copies?

An hon. Member: One thousand copies.

The Chairman: One thousand copies?

M. Lachance: Croyez-vous avoir besoin de 1,000 exemplaires? Qu'en pensez-vous? Quelle est la demande?

Le président: Il s'agit du minimum. Or, nous voulions disposer du minimum mais avant de commencer, et la quantité que nous pouvions obtenir, était 1,000 exemplaires, que cela nous plut ou non.

M. Lachance: C'est bien, va pour 1,000 exemplaires.

The motion is carried.

The Chairman: Now, a motion to give a title to . . . un nom au Sous-comité.

Je propose que le Comité porte le titre de Sous-comité sur les infractions commises à l'aide d'ordinateurs du Comité permanent de la justice et des questions juridiques.

Des voix: D'accord.

M. Robinson (Etobicoke—Lakeshore): De quoi s'agit-il . . .

Le président: Le Sous-comité sur les infractions commises à l'aide d'ordinateurs.

M. Robinson (Etobicoke—Lakeshore): Non, non. Ma question s'adresse au président. J'aimerais connaître le mandat du Comité. Le titre est-il tiré de ce mandat?

M. Lachance: Il s'agit du sujet traité par le projet de loi de M. Beatty.

M. Beatty: Il s'agit donc des infractions commises à l'aide d'ordinateurs.

[Texte]

Mr. Lachance: Which is computer crime.

Mr. Robinson (Etobicoke—Lakeshore): That is broad enough in its scope then, is it, to cover the subject?

The Chairman: We did that with my own private member's bill on profit sharing and there was no problem whatsoever.

Le président: J'ai besoin maintenant d'une motion concernant la comparution des témoins: M. Lachance propose:

Que le président soit autorisé à prévoir des séances et à prendre des dispositions pour la comparution des témoins après les consultations avec les autres membres du Sous-comité.

La motion est adoptée.

Le président: Motion relative aux dépenses des témoins:

-Que, lorsqu'un témoin en fait la demande, des frais raisonnables de déplacements et de séjour soient versés aux témoins invités à comparaître devant le Sous-comité concernant son Ordre de renvoi.

Simplement un bref commentaire: je suggère que les frais raisonnables de déplacements et de séjour soient à la charge du Comité seulement si nous invitons des gens et que si des gens demandent à comparaître; à moins d'accord de tous les membres, les frais sont défrayés par les témoins qui voudront être entendus. Mais lorsque nous demanderons des témoins, pour ces témoins-là, en fin de compte, des frais raisonnables leur seront remboursés.

M. Lachance: De toute façon, madame le président, je présume que vous n'entendrez pas de témoin à moins d'ententes. Alors je ne sais pas si le problème se pose vraiment.

The Chairman: I will speak English for that. In the previous subcommittee I chaired on profit sharing, the people wanted to be heard and wanted us to pay their expenses. It was a case-by-case approval, but when we were inviting people at our own request then it was understood that, of course, the committee was agreeing to cover reasonable expenses—when we were inviting them and we were agreeing on the list of people we would ask to appear before the committee.

• 1740

Mr. Beatty: Agreed. But I do not think there is any requirement that there be unanimity. If the committee itself decides—I assume we will function by consensus—we are likely not even to have a voting in writing the report.

The Chairman: No, but since we are reporting to this committee, and of course the expenses can be very large, if you have a large number of witnesses, and to understand that . . .

Mr. Lachance: To ensure the judgment of the subcommittee, I think a case-by-case approach is the proper one in a case like that.

[Traduction]

M. Lachance: Les infractions commises à l'aide d'ordinateurs.

M. Robinson (Etobicoke—Lakeshore): Cela est donc assez vaste pour englober le sujet?

Le président: Nous avons fait la même chose lorsque j'ai présenté mon projet de loi relatif au partage des bénéfices, et cela n'a entraîné aucun problème.

The Chairman: I now need a motion concerning the hearing of witnesses: Mr. Lachance moves the following:

That the chairman be authorized to call meetings and to make the necessary arrangements to have witnesses appear before the sub-committee after consultation with other members of the sub-committee.

The motion is carried.

The Chairman: Now, a motion concerning the witnesses' expenses:

That, when requested by the witness, reasonable travelling and living expenses be paid to witnesses who are invited to appear before the sub-committee in relation to its order of reference.

Here, I have a brief comment to make. I propose that reasonable travelling and living expenses be paid by the committee only if we have invited the witnesses; if they are the ones who have asked to be heard, unless we have unanimous agreement among members, they will have to pay their own expenses themselves. However, when we will ask witnesses to come here, we will pay them reasonable travelling and living expenses.

Mr. Lachance: Anyway, Madam Chairman, I suppose that you will not hear witnesses unless there is an agreement, and if this is the case, I do not think a problem would arise.

Le président: Je vais m'exprimer en anglais là-dessus. Lorsque j'ai été présidente du Sous-comité portant sur le partage des bénéfices, les gens voulaient venir témoigner tout en nous demandant de leur rembourser leurs frais de déplacement. Nous avons donc décidé d'étudier chaque demande séparément avant de l'approuver, mais lorsque c'était nous qui invitions des témoins, il était entendu que le Comité allait rembourser les frais de déplacement et de séjour de ces derniers. C'est donc ce que nous faisons lorsque c'est nous qui les invitions, qui établissons la liste de ceux qui allaient comparaître.

M. Beatty: D'accord. Je ne crois pas toutefois qu'il soit nécessaire d'obtenir l'unanimité. Si le Comité souhaite que nous adoptions la règle du consensus, il est probable que nous n'aurons même pas à voter pour la rédaction du rapport.

Le président: En effet, mais puisque nous devons faire rapport au Comité et qu'il est évident que les dépenses seront très importantes, s'il y a beaucoup de témoins et si . . .

M. Lachance: Je crois que dans un cas semblable le meilleur moyen serait d'envisager les situations au fur et à mesure.

[Text]

The Chairman: Okay.

Est-ce que, monsieur Lachance, vous faites la proposition que l'on couvrira les dépenses de ceux qui seront invités à comparaître, pourvu que les frais de séjour et de déplacement soient raisonnables? Cela va?

Now we have to deal with the time schedule and business of the subcommittee.

Mr. Lachance: May I suggest that maybe the subcommittee will want to have informal discussions about its schedule. The only requirement that is enshrined, if you want, is that you have to make a progress report of some sort by March 31 to the full committee. So you organize your work in view of that. I said a progress report; it is a report.

Mr. Beatty: By March 31.

Mr. Lachance: March 31; that is why I was eager that this subcommittee be organized, so that you can start your work and, at some point, tell the full committee where you are, what you want to do, what is your progress, and what is your deadline for a definitive report.

Mr. Beatty: We could perhaps have an informal meeting tomorrow morning to plan agenda . . .

The Chairman: I will not be here, but since we . . .

Mr. Lachance: We can cover it now, if you want.

The Chairman: I will be here on Monday.

Mr. Beatty: Unfortunately, I will not be here on Monday because I have to speak in Toronto.

Mr. MacBain: Well, when we adjourn tonight we could have a steering committee meeting.

Mr. Hnatyshyn: Why do you not meet right after this . . . ?

Mr. Beatty: I have to speak in the House at 6.00 p.m.

Mr. Hnatyshyn: You can start your discussions and see how far you get.

Mr. Beatty: What time are you leaving?

The Chairman: Now. Two persons have been waiting for me for an hour.

Mr. Beatty: Well, I think there is some urgency that we get going on it because of the fact that the government House Leader indicated this session could end within a couple of weeks, in response to Ray.

Mr. Lachance: Why do you not have a full-fledged meeting Tuesday some time, and then finish off your . . . ? You can discuss your work and start working on it.

The Chairman: We have already reserved for Tuesday 9.30 a.m., 11.00 a.m. and 3.30 p.m., because of the committee at large, just to study the report on prostitution.

Mr. Lachance: You organize your work.

[Translation]

Le président: D'accord.

Mr. Lachance, are you moving that we cover reasonable travelling and hotel expenses for our witnesses?

Il nous faut maintenant nous occuper du calendrier et du programme du Sous-comité.

M. Lachance: Puis-je suggérer que le Sous-comité discute librement de son programme avec la seule réserve qu'il présente un rapport intérimaire d'ici le 31 mars au comité plénier? Cela vous permet d'organiser votre travail dans la perspective d'un rapport intérimaire donc véritablement d'un rapport.

M. Beatty: Avant le 31 mars.

M. Lachance: Oui; c'est pourquoi je voulais que le Sous-comité s'organise et commence immédiatement à travailler afin de pouvoir dire un jour au comité plénier où il en est, ce qu'il souhaite faire, ce qu'il a réalisé et à quelle date il entend déposer un rapport définitif.

M. Beatty: Nous pourrions peut-être ainsi nous réunir entre nous demain matin pour prévoir notre calendrier . . .

Le président: Je ne serai pas là mais étant donné que . . .

M. Lachance: Si vous voulez, nous pouvons en parler aujourd'hui.

Le président: Je serai ici lundi.

M. Beatty: Malheureusement, je ne serai pas là, car je dois être lundi à Toronto.

M. MacBain: Pourquoi ne pas envisager une réunion du comité directeur à l'ajournement ce soir?

M. Hnatyshyn: Pourquoi ne vous réunissez-vous pas tout de suite après . . . ?

M. Beatty: Je dois parler à la Chambre à 18h00.

M. Hnatyshyn: Vous pouvez commencer à discuter et voir où vous en êtes.

M. Beatty: À quelle heure vous en allez-vous?

Le président: Maintenant. Il y a deux personnes qui m'attendent depuis une heure.

M. Beatty: Je crois qu'il est urgent que nous démarrions car le leader de la majorité à la Chambre a déclaré à Ray que la session pourrait prendre fin d'ici deux semaines.

M. Lachance: Pourquoi ne pas avoir une véritable réunion mardi à un moment donné pour terminer . . . Vous pouvez discuter de votre travail et démarrer tout de suite.

Le président: Nous avons déjà réservé mardi à 9h30, 11h00 et 15h30, car le comité plénier doit étudier le rapport sur la prostitution.

M. Lachance: Vous organisez votre travail comme vous l'entendez.

[Texte]

The Chairman: No, but as I say, I already have that timeframe, but I just want to consult with you, not to hold the subcommittee during the same time the main committee is sitting.

Mr. Lachance: As far as possible . . .

The Chairman: Especially, as far as prostitution is concerned. I have . . .

Mr. Lachance: No, no, prostitution is not next week; prostitution is the week after.

The Chairman: The week after.

Mr. Lachance: Yes.

The Chairman: So, how about . . . ?

Mr. Beatty: Could we then confer by telephone tomorrow? You and Ken and I could confer by telephone.

The Chairman: Okay. I have a difficulty with all sorts of stuff too. I am going to the Toronto Stock Exchange for a visit tomorrow morning, and that is my . . .

Mr. Robinson (Etobicoke—Lakeshore): Let us decide now that we will meet Tuesday at 9.30 a.m. How is that?

Mr. Hnatyshyn: Have you got recommended witnesses right now, or anybody . . . ?

Mr. Lachance: During that time, why does not each one of the members draft a list of witnesses that he or she thinks will be good witnesses so that we can . . . ?

Mr. Beatty: Unfortunately, for me, depending on how late the speech goes on Monday night, I may have to drive in on Tuesday morning.

The Chairman: Tuesday afternoon will be fine with me, 3.30 p.m.?

Mr. Beatty: At 3.30 p.m. we have our meeting. Let us say 5.00 p.m.

The Chairman: Fine.

Mr. Robinson (Etobicoke—Lakeshore): Okay.

Mardi prochain.

The Chairman: Okay; 5.00 p.m.

Mr. Lachance: May I suggest that, as I said, you have your list of witnesses ready for that time, and then you can agree and start calling them?

The Chairman: Yes.

Mr. Robinson (Etobicoke—Lakeshore): Okay. So have a notice sent to us for 5.00 p.m. on Tuesday.

Mr. Beatty: With the Clerk of the Committee.

Mr. Lachance: Mr. de Champlain will be the Clerk of the Committee.

Mr. Robinson (Etobicoke—Lakeshore): How many members are there on this committee?

The Chairman: Four.

[Traduction]

Le président: Je répète que j'ai déjà réservé ces heures et c'est pourquoi j'aimerais que les réunions du Sous-comité ne se passent pas au même moment.

M. Lachance: Dans la mesure du possible . . .

Le président: Surtout pour ce qui est de la prostitution. J'ai . . .

M. Lachance: Non, la prostitution ce n'est pas pour la semaine prochaine mais pour la semaine d'après.

Le président: La semaine d'après.

M. Lachance: Oui.

Le président: Alors, que pensez-vous . . . ?

M. Beatty: Pourrions-nous alors nous téléphoner demain? Ken, vous et moi pourrions en reparler au téléphone.

Le président: D'accord. J'ai également des tas de choses. Je vais à la Bourse de Toronto demain matin et c'est . . .

M. Robinson (Etobicoke—Lakeshore): Décidons donc maintenant que nous nous réunirons mardi à 9h30. Qu'en pensez-vous?

M. Hnasysyn: Avez-vous des témoins qui ont déjà été recommandés ou quelqu'un . . . ?

M. Lachance: D'ici là pourquoi chacun des membres ne dresse-t-il pas une liste des témoins qu'il voudrait entendre de sorte que nous puissions . . . ?

M. Beatty: Malheureusement, je ne sais pas à quelle heure mon discours se terminera lundi soir, mais je risque d'être obligé de n'arriver que mardi matin en voiture.

Le président: Mardi après-midi me conviendrait, à 15h30?

M. Beatty: À 15h30, nous avons notre réunion. Disons 17h00.

Le président: D'accord.

M. Robinson (Etobicoke—Lakeshore): D'accord.

On Tuesday.

Le président: D'accord, 17h00.

M. Lachance: Puis-je suggérer que vous prépariez une liste de témoins pour cette réunion, de sorte que vous puissiez vous mettre d'accord sur ceux que vous souhaitez inviter?

Le président: D'accord.

M. Robinson (Etobicoke—Lakeshore): Très bien. Alors envoyez-nous un avis de convocation pour 17h00 mardi.

M. Beatty: Le greffier du Comité s'en chargera.

M. Lachance: M. de Champlain sera greffier du Comité.

M. Robinson (Etobicoke—Lakeshore): Combien y a-t-il de membres à ce Comité?

Le président: Quatre.

[Text]

Mr. Beatty: Will we have quorum problems with having alternates there?

Mr. Lachance: No, we will not have any problems because both Mr. Hnatyshyn and I... we are here only for technical reasons. Actually, you are the member from your caucus. Mr. Robinson and I...

Mr. Beatty: We automatically substitute in your absence.

Mr. Lachance: Yes, but I do not think I am going to be here a lot, not because I am not interested...

Mr. Beatty: No, no.

Mr. Lachance: —but because of the full committee.

Mr. Beatty: But we will automatically be substituting; there is no problem with somebody saying, okay...

Mr. Lachance: You are the designated alternates.

Mr. Beatty: Okay.

Mr. Lachance: It is a new form invented for you. It does not exist in law, but for the sake of the committee, you are the alternate and Mr. Robinson is the alternate.

The Chairman: Since what the witnesses say will be printed... I think that motion too is prevented...

• 1745

Mr. Lachance: It would be normal. It would be a bit strange to have only the chairperson and no members of the committee to hear witnesses. I think, because it is a committee of four, rather than pass that motion that we can hear witnesses without having a quorum, I think you should try to have a rule of thumb that we should have at least two members to hear witnesses.

Mr. Beatty: I think we can operate very informally among ourselves, as long as we do not run into problems that somebody from the House comes descending on us to announce the whole process as being illegal.

The Chairman: Thank you. Before closing the meeting, may I introduce Madam Hébert. She is the parliamentary research assistant who will help this committee put all the information together and will be supporting our work.

Mr. Robinson (Etobicoke—Lakeshore): Madam Chairman, could she have some material ready for us, say, by Monday or Tuesday morning?

Le président: Est-ce que vous avez des choses de prêtes pour mardi prochain?

Mr. Lachance: May I speak on this point? Mr. Beatty has had his own document, which is quite comprehensive, distributed to all members of the committee, so you shall have that if you want it.

Mr. Robinson (Etobicoke—Lakeshore): Yes, I have that document. I also have some clippings from the library. But I wondered if there was anything else. For instance, I am wondering particularly if there was any information available

[Translation]

M. Beatty: Y aura-t-il des problèmes de quorum et de remplaçants?

M. Lachance: Non, il n'y aura pas de problèmes, car M. Hnatyshyn et moi-même ne sommes ici que pour des raisons techniques. En fait, vous êtes le représentant de votre caucus. M. Robinson et moi...

M. Beatty: Nous vous remplaçons automatiquement.

M. Lachance: Oui, mais je ne pense pas que je serai beaucoup là, non que cela ne m'intéresse pas...

M. Beatty: Non, bien sûr.

M. Lachance: ... Mais parce que je serai occupé par le comité plénier.

M. Beatty: Mais nous serons automatiquement vos remplaçants; il n'y a pas de risque que quelqu'un dise...

M. Lachance: Vous êtes les substituts désignés.

M. Beatty: D'accord.

M. Lachance: C'est une nouvelle formule inventée pour vous. Cela n'existe pas en droit mais pour le Comité, vous êtes le remplaçant et M. Robinson l'est aussi.

Le président: Étant donné que ce que disent les témoins sera imprimé, je pense que l'on ne peut pas non plus présenter cela sous forme de motion...

M. Lachance: Ce serait normal car il est difficile d'imaginer que seule la présidence puisse entendre des témoins. Étant donné qu'il s'agit d'un comité de quatre personnes, il est mieux que la règle soit de prévoir que l'on entende des témoins à condition qu'il y ait deux membres du Comité présents plutôt que d'adopter une motion permettant d'entendre les témoins sans quorum.

M. Beatty: Je crois qu'il est en effet possible de fonctionner très librement à condition que nous ne rencontrions pas de problème, que quelqu'un de la Chambre n'arrive pas pour nous annoncer que tout ce que nous faisons est illégal.

Le président: Merci. Avant de terminer, je voudrais vous présenter M^{me} Hébert qui est la documentaliste parlementaire qui nous aidera à compiler les informations obtenues et à effectuer notre travail.

M. Robinson (Etobicoke—Lakeshore): Madame le président, pourrait-elle nous préparer quelque chose pour lundi ou mardi matin?

The Chairman: Will you have anything ready for Tuesday?

M. Lachance: Puis-je dire un mot à ce sujet? M. Beatty a un document tout à fait complet qu'il a fait distribuer à tous les membres du Comité si bien que vous pouvez l'obtenir si vous le souhaitez.

M. Robinson (Etobicoke—Lakeshore): Oui, j'ai en effet ce document. J'ai également certains articles fournis par la Bibliothèque. Je me demandais simplement s'il pouvait y avoir autre chose. En particulier, s'il existe des informations que

[Texte]

from some of the computer companies and the banks and so on, because there have been complaints of theft from computer banks, data banks and so on. So I just wonder if some of this is readily available.

Mr. Beatty: Maybe what you could do is touch bases with my office and we would gladly make available anything in our files for you.

Mr. M. P. Rosen (Researcher): Madam Chairman, with your permission, we have some large articles which we have collected already, and which we can make available to members if they wish, of some of the important cases which have come down recently.

Mr. Beatty: Anything in my files is certainly available.

Mr. Robinson (Etobicoke—Lakeshore): You are speaking of court cases, are you?

Mr. Rosen: Yes.

The Chairman: Anyway, whatever information is available can just be shared by the members of the committee.

Mr. Robinson (Etobicoke—Lakeshore): Could the headnotes be made available, even if we do not have all the transcripts?

Mr. Rosen: Yes.

The Chairman: Thank you, the meeting is adjourned to the call of the Chair.

Tuesday, March 15, 1983

• 1710

The Chairman: We can just manage to organize our work. I was talking to the clerk and he was saying that some people would be ready and willing to appear before our committee next week. He suggested RCMP experts in the commercial crime branch would be willing to testify next week, which is of course short notice but they can. And also Mr. Galen Duncan for the Director of the Canadian Centre for Judicial Statutes, who would give us an overview of what could be done or maybe should be done and that could not be done. The Canadian Business Equipment Manufacturers' Association, I believe probably related more or less to the hardware, would be willing also to . . .

Mr. Robinson (Etobicoke—Lakeshore): Who would be their representative?

The Chairman: We do not have the name, but I just presume—James Flood?

Mr. Beatty: CBEMA is part of the release on computer crime dated March 30. It is not just hardware they are dealing with but rather with what the head of CBEMA calls "the new sanctions against computer abuse", so they are concerned about the issue.

[Traduction]

pourraient nous fournir des sociétés d'informatique, des banques, etc., car on s'est plaint de vols de banques d'information, de banques de données, etc. Je me demandais simplement s'il y avait quelque chose qui existait déjà.

M. Beatty: Peut-être pourriez-vous contacter mon bureau car nous serons ravis de vous communiquer tout ce que nous avons accumulé.

M. M. P. Rosen (documentaliste): Madame le président, si vous permettez, nous avons quelques longs articles que nous pourrions mettre à la disposition des députés car ils portent sur certains des cas importants dont on a récemment parlé.

M. Beatty: Tout ce que j'ai dans mes dossiers est également à votre disposition.

M. Robinson (Etobicoke—Lakeshore): Vous parlez des affaires présentées aux tribunaux, n'est-ce pas?

M. Rosen: Oui.

Le président: De toute façon, les membres du Comité peuvent se partager tous les renseignements à leur disposition.

M. Robinson (Etobicoke—Lakeshore): Pourrait-on avoir au moins tous les titres même si les textes ne sont pas complets?

M. Rosen: Oui.

Le président: Merci, la séance est levée.

Le mardi 15 mars 1983

Le président: Nous arrivons tout juste à nous organiser. Je viens justement de parler au greffier, qui me dit qu'il y aurait des gens prêts à comparaître la semaine prochaine . . . ce qui ne leur laisse pas beaucoup de temps, évidemment, mais ils disent pouvoir le faire . . . devant ce Comité. Il a mentionné, entre autres, les spécialistes de la Section des infractions commerciales de la GRC, ainsi que M. Galen Duncan, représentant le directeur du Centre canadien de la statistique juridique, qui pourrait nous donner une idée de ce qui pourrait, qui devrait être ou ne devrait pas être fait. L'Association canadienne des fabricants d'équipement de bureau serait également disposée à comparaître, mais elle s'intéresse davantage au matériel proprement dit.

M. Robinson (Etobicoke—Lakeshore): Qui serait son représentant?

Le président: Nous ne le savons pas, mais je crois qu'il s'agit de James Flood.

M. Beatty: L'Association canadienne des fabricants d'équipement de bureau figure dans le communiqué sur les infractions relatives aux ordinateurs, qui est daté du 30 mars. Elle ne s'intéresse pas qu'au matériel, elle s'occupe également de ce que son directeur appelle «les nouvelles sanctions contre

[Text]

The Chairman: And we have the list prepared by the Library of Parliament research office. Do you have a list?

Mr. Beatty: Yes.

The Chairman: Well, I would suggest that since some are really related and familiar with the subject matter and do not have to have travelling problems, they could be called for next week. So I interpret that we might start with the RCMP. I would feel comfortable because they have an overview of what has been done in other countries of the world and they have a very pragmatic approach and could give some suggestions about what they did also.

So my suggestion would be that we start with them and we will probably be more in the theory side of the problem, but I would feel that we would have an overview of the practical approach if the RCMP were the first witnesses.

Mr. Robinson (Etobicoke—Lakeshore): I would think at the beginning that we would want not only what they can tell us—that is kind of after the fact. I would like to know from the computer industry how the crimes can be perpetrated; what kind of crimes are we actually talking about? This is the kind of overview I think we need first and then we can decide who we want to zero in on.

The Chairman: Yes, but I am talking about an expert on that. I am not talking about people who just investigate; I am talking about someone who is familiar with the techniques as well. First of all, what do they face in reality when they have a crime being committed? Then we might be able to approach it in a more pragmatic way than just trying to find a theory that would not, in fact, correct the problems.

Mr. Beatty: I just have two other suggestions. I think the work has been done by the Library of Parliament is excellent and the clerk has already started to contact people. I am very pleased at that. But I think we should hear either from the Minister of Justice or from his officials as to what they have in mind.

The Chairman: Yes, I think they could be in next week, too. Oh, this week they can be available.

Mr. Beatty: That would be fine, from my point of view, Madam Chairman.

The Chairman: They are available on Thursday? Okay. Yes, they are available; are you available?

Mr. Beatty: What time would that be?

The Chairman: Would you be available at 9:30 this Thursday?

[Translation]

les abus relatifs aux ordinateurs», ce qui montre bien que le problème les préoccupe.

Le président: Nous avons également la liste préparée par le bureau de recherche de la Bibliothèque du Parlement. Est-ce que vous avez la liste?

M. Beatty: Oui.

Le président: Je proposerais donc, puisque certains de ces témoins connaissent bien le sujet et n'ont pas à se déplacer, que nous pourrions les convoquer pour la semaine prochaine. Nous pourrions donc commencer par la GRC, qui me paraît tout indiquée, car elle a une vue d'ensemble de ce qui se pratique dans les autres pays, elle a une méthode d'approche très pragmatique et pourrait également nous communiquer certaines des mesures qu'elle a prises.

Je propose donc que nous commençons par la GRC, qui aborderait probablement la question sous un angle plus théorique, mais, avec ce premier témoin, nous aurions une notion d'ensemble des mesures pratiques à envisager.

M. Robinson (Etobicoke—Lakeshore): Ce que peut nous dire la GRC ne me paraît pas une introduction suffisante, car elle s'intéresse aux mesures de répression plutôt que de prévention. J'aimerais apprendre de l'industrie des ordinateurs comment les infractions peuvent être commises, et de quel genre d'infractions nous parlons au juste. C'est là le genre de perspective que nous aimerions avoir en préambule, après quoi nous pourrions décider du champ précis de notre action.

Le président: Oui, mais je vous parle là d'un spécialiste, non de gens qui font simplement des enquêtes. La personne en question connaît également à fond les techniques. Tout d'abord, comment la situation se présente-t-elle lorsqu'une infraction a été commise? Nous pourrions alors étudier la question de façon plus pratique plutôt que de nous familiariser avec des théories qui ne remédieraient pas en réalité aux problèmes.

M. Beatty: J'ai deux autres propositions. La Bibliothèque du Parlement a fait un excellent travail et le greffier a déjà pris contact avec des gens. C'est très bien. Et je crois que nous devrions être informés par le ministre de la Justice ou par ses collaborateurs de leurs intentions.

Le président: Oui, je crois qu'ils pourraient également comparaître la semaine prochaine. Ou même cette semaine.

M. Beatty: Ce serait très bien, à mon avis, madame le président.

Le président: Ils seraient donc disponibles jeudi? Très bien. Oui, ils sont disponibles; l'êtes-vous aussi?

M. Beatty: À quelle heure?

Le président: Seriez-vous libre ce jeudi à 9h30?

• 1715

Mr. Beatty: Well, I cannot. The broadcasting committee, the Committee on Communications and Culture, has

M. Beatty: Eh bien, je ne pourrai pas. Le comité chargé des questions de radiodiffusion, c'est-à-dire le Comité des communications et de la culture, est saisi du rapport Applebaum-

[Texte]

Applebaum-Hébert before us. If I am not going to be there . . . What about Thursday afternoon?

The Chairman: Thursday at 3:30?

Mr. Beatty: 3:30 is fine for me.

Mr. Robinson (Etobicoke—Lakeshore): I have not got my list here so I cannot tell you at the moment.

The Chairman: Let us make a try for it because we have to phone them and ask them to be here.

Mr. Robinson (Etobicoke—Lakeshore): I will let you know as soon as I go back to my office.

Mr. Beatty: Yes, 3:30 would be fine for me, although I may have to leave early.

The other person that I had in mind as a possible other person to add was Professor David Flaherty from the University of Western Ontario. He is in the History Department there and he is perhaps the academic who has done more work on privacy than anyone else, and there is a very strong privacy component to the computer crime.

The Chairman: Well, do you want to . . . ? It all depends, you know, if we want to hear all those who are listed here and then it is just a matter of calling and trying to fit them into our agenda, or do you want to prioritize? I know there is a human rights aspect to it, but my impression was that . . . I would not say that is the last thing, but I think the practicality is that if we know exactly the problem from a very technical point of view, then it is easier to come to grips with the human rights aspect of it, and, of course, the possibility of how to be efficient at making sure that we do not suggest any abuse in that direction, but simply . . .

Mr. Robinson (Etobicoke—Lakeshore): Could we not request that if all of these people are to be considered or have indicated that they are interested . . . or maybe they have not, maybe this is just the Library's list—I do not know at the moment whether these people have been contacted and if they are actually interested in appearing before the committee. If they are interested in appearing then I . . . Some of them are going to be covering the same as others and I think they should be lumped together. Apart from that, it seems to me that the main computer firms are not actually represented. For instance, why is there not somebody from IBM on the list?

The Chairman: I depends on the Canadian Business Equipment Manufacturers' Association to call upon one manufacturer instead of another one . . . I would at least ask the view from the industry in general and then if we feel that we should meet one specific company . . . I just feel that it would be a little bit awkward for us to ask for one and . . .

Mr. Robinson (Etobicoke—Lakeshore): Well, we could ask for one in the large computer business; certainly the largest and the most extensive and the the company that sells more computers than any other company. You could ask for people in the small computer businesses . . . the mini-computers like Timex or somebody, you know.

[Traduction]

Hébert. Si je n'y vais pas . . . Que diriez-vous de jeudi après-midi?

Le président: Jeudi à 15h30?

M. Beatty: 15h30 me convient tout à fait.

M. Robinson (Etobicoke—Lakeshore): Je n'ai pas ma liste en main, je ne puis donc pas vous dire ce qu'il en est pour le moment.

Le président: Essayons car nous devons leur téléphoner et leur demander de venir.

M. Robinson (Etobicoke—Lakeshore): Je vous ferai savoir aussitôt que je serai de retour à mon bureau.

M. Beatty: Oui, 15h30 me conviendrait tout à fait, bien que je sois peut-être obligé de partir tôt.

L'autre personne à laquelle je pensais comme témoin est le professeur David Flaherty de l'Université Western Ontario. Il y enseigne l'histoire et est peut-être celui qui a effectué le plus de travail sur l'aspect privé de certaines choses, et justement, les infractions en matière d'ordinateur comportent un aspect privé très important.

Le président: Eh bien, voulez-vous . . . ? Cela dépend, vous savez, si nous voulons entendre tous les témoins figurant sur la liste ici, il ne s'agira que de leur téléphoner et essayer de les inscrire à notre ordre du jour, à moins que vous ne vouliez indiquer des priorités. Je n'ignore pas que cette question touche aux droits de la personne, mais j'ai eu l'impression que . . . Je ne considère pas cela comme la chose la moins importante, mais je crois que si nous maîtrisons assez bien l'aspect technique de cette question, alors il sera d'autant plus facile de saisir ce qui touche aux droits de la personne, et partant, bien entendu, d'être plus efficace lorsqu'il s'agira de décourager toute infraction dans ce sens, mais simplement . . .

M. Robinson (Etobicoke—Lakeshore): J'ignore si toutes ces personnes veulent venir témoigner, car il s'agit peut-être seulement de la liste de la bibliothèque, mais si on les a rejointes et si elles sont intéressées à venir alors . . . Certaines d'entre elles aborderont les mêmes questions que d'autres, et je crois donc qu'il faudrait les regrouper. À part cela, il me semble que les principaux fabricants d'ordinateurs ne sont pas représentés. Par exemple, pourquoi n'y a-t-il pas de représentant de la compagnie I.B.M. sur la liste?

Le président: C'est à l'Association canadienne de fabricants d'équipement de bureau qu'il revient de désigner un fabricant plutôt qu'un autre . . . Cependant, je crois qu'il faudrait entendre l'avis de l'industrie en général, et peut-être rencontrer les représentants d'une entreprise précise . . . J'estime tout simplement qu'il serait peut-être un peu gauche de notre part d'en inviter une et . . .

M. Robinson (Etobicoke—Lakeshore): Eh bien, nous pourrions demander à l'une des grandes entreprises de venir, tout au moins la plus grande et celle qui vend le plus d'ordinateurs que toutes les autres. En outre, on pourrait faire comparaître des représentants des petites entreprises

[Text]

Mr. Beatty: CBEMA represents them also. It is a trade association.

The Chairman: Yes, that is my impression.

Mr. Robinson (Etobicoke—Lakeshore): I know, but you see, what I want to do is to zero in on what happens . . . how do we happen to have computer crime? What are they doing to combat this or to avoid it?

Mr. Beatty: CBEMA would be able to answer from a technological point of view.

The Chairman: Well, let us start with this one and we then if we need to see one company in particular or some companies . . . there is one body from the government—or I mean, it is outside of government but it is related to the Canadian government, that is the National Council Research. I think they are actually undergoing some study, that is some of the vibes I got, that I have not seen the National Research Council . . .

Mr. Robinson (Etobicoke—Lakeshore): What number is that on the list?

The Chairman: I have not seen the name on the list unless someone is related to the *Conseil national de la recherche*. I was told that they are doing some research on that, that they already have a group and they have expertise; it is a group made up of private and companies in various sectors that are working with the NRC. So I would say that also they have already some work in progress and they could probably share their work with us.

Mr. Beatty: Sure. I think that is a good idea. I think, along the lines of what Ken was talking about, that CBEMA should be an early witness.

The Chairman: Yes, I do agree.

Mr. Beatty: Also, I think you would find that another person on the security aspect of it and the technology is number 10, Jim Finch, from Jim Finch and Associates. He is extremely knowledgeable on the technology aspects and might be useful.

• 1720

Mr. Robinson (Etobicoke—Lakeshore): Do we have any on the list from, say, the United States or the U.K. or something? Do you think there is anybody that has some experience in the field already that we could learn from and not have to recreate the wheel?

The Chairman: Well, for the U.S. I think what my suggestion would be is to wait for the RCMP because they are in

[Translation]

d'informatique . . . celles qui fabriquent les mini-ordinateurs comme les Timex.

M. Beatty: L'Association canadienne des fabricants d'équipement de bureau les représente elles aussi. C'est une association professionnelle.

Le président: Oui, c'est aussi mon impression.

M. Robinson (Etobicoke—Lakeshore): Je le sais mais vous voyez, j'aimerais me concentrer sur ce qui se passe . . . savoir comment se produisent les infractions en matière d'ordinateurs. J'aimerais aussi savoir ce que font les entreprises pour empêcher ce genre de choses ou pour les combattre?

M. Beatty: L'A.C.F.E.B. sera en mesure de répondre à cela sur le plan technique.

Le président: Eh bien, commençons par cela, et voyons ensuite s'il est nécessaire de faire témoigner une entreprise particulière ou certaines entreprises . . . par ailleurs, il existe un organisme gouvernemental appelé le Conseil national de recherches. Or, d'après ce que j'ai entendu dire, il effectue présentement une étude, que je n'ai cependant pas consultée.

M. Robinson (Etobicoke—Lakeshore): Où cet organisme figure-t-il sur la liste?

Le président: Je n'ai pas vu son nom sur la liste, à moins que quelqu'un n'ait des liens quelconques avec le Conseil national de recherches. Enfin, on m'a dit que cet organisme effectue une recherche quelconque sur le sujet, qu'il dispose donc d'un groupe de spécialistes. Ces derniers représentent l'entreprise privée oeuvrant dans divers secteurs en collaboration avec le Conseil national de recherches. Son travail est donc probablement déjà en chantier, et il pourrait probablement en partager les données avec nous.

M. Beatty: Certainement. Cela me paraît une bonne idée. Par ailleurs, je suis d'accord avec ce que Ken disait au sujet de l'Association canadienne des fabricants d'équipement de bureau, c'est-à-dire que cet organisme devrait être un des premiers à témoigner.

Le président: Oui, je suis d'accord.

M. Beatty: Par ailleurs, il y a quelqu'un d'autre qui peut témoigner au sujet de l'aspect sécurité et technologie, il s'agit de M. Jim Finch de *Jim Finch and Associates*, figurant au numéro 10. Il s'y connaît beaucoup en matière de technologie et pourrait peut-être nous être utile.

M. Robinson (Etobicoke—Lakeshore): De ceux qui figurent sur ma liste, y en a-t-il qui soient des États-Unis, des Royaume-Uni ou d'ailleurs? Croyez-vous qu'il existe quelqu'un ayant déjà une certaine expérience dans ce domaine et qui puisse nous renseigner afin que nous ne soyons pas obligés de réinventer la roue?

Le président: Eh bien, pour ce qui est des États-Unis, je vous propose d'attendre l'avis de la G.R.C. là-dessus, car la Gendarmerie est en contact étroit avec d'autres services

[Texte]

close contact with other police administrations, and they might have some suggestions.

Mr. Robinson (Etobicoke—Lakeshore): Well, that is good. I was thinking of maybe the FBI or the CIA or . . .

The Chairman: Yes, but before calling them all, I think if we can have the expertise from our own people, I do not think we . . . it would save time.

Mr. Beatty: I would think, in any case, that the parliamentary secretary indicated the Department of Justice has been in contact with the Americans in a number of jurisdictions, and it may be that we will get some leads from them as to what is happening.

The Chairman: So we have actually the Department of Justice for this week, and for next week we might ask CBEMA. The RCMP—that would make the first three witnesses, and then we could go along . . . I mean, other . . . maybe you could on Thursday give me your reactions about which others could be called.

Mr. Beatty: Right.

The Chairman: Is this agreeable to you?

Because the Bar will come and others will come but in order to clarify the issue a little bit familiarize ourselves with those who really are in the field, I believe that with Justice, the RCMP and CBEMA we have a good start and the other ones . . . There are two professors from Western Ontario. I believe that but I do not consider them as *two* witnesses; probably the two could be invited at the same time, or one or the other.

Mr. Robinson (Etobicoke—Lakeshore): Can you tell us when we have to report our findings and make our recommendations? Secondly, will this committee continue into the next session, or will we have to get special terms of reference to have it referred over to the next session? Because obviously we could never see all these witnesses between now and then.

The Chairman: It all depends on your recommendation. As far as I am concerned, my feeling was that once we establish our schedule and we want to hear some witnesses on March 30, where we have to report would be just to be updating the main committee on where we are and ask for an extension and wait until we know where we are going. I cannot presume anything about when the session is going to end. If we have to refer the same question, the same subject matter, in the next session, we will think about it when we are there, but right now I just suggest that we work in an orderly manner and do as much as we can until March 30, and then we continue and ask the main committee to continue our work.

Mr. Robinson (Etobicoke—Lakeshore): But is it your intention that we will a report before the House adjourns?

[Traduction]

policiers, elle pourra peut-être donc nous proposer certaines choses.

M. Robinson (Etobicoke—Lakeshore): Très bien. Je songeais peut-être au F.B.I. ou à la C.I.A. ou . . .

Le président: Oui, mais avant de faire comparaître tous ces gens-là, ce serait une bonne chose de bénéficier des lumières de nos propres services; je ne crois pas que . . . Cela nous ferait gagner du temps.

M. Beatty: De toute façon, je crois que le secrétaire parlementaire a laissé savoir que le ministère de la Justice a été en contact avec les Américains de divers services, et il se peut que ces derniers nous donnent une idée de ce qui se passe.

Le président: Donc, cette semaine nous recevrons le ministère de la Justice, et la semaine prochaine nous demanderons peut-être à l'Association canadienne des fabricants d'équipement de bureau de venir témoigner. La G.R.C. enverra trois témoins, après quoi nous pourrions poursuivre . . . j'entends par là d'autres . . . peut-être que jeudi vous pourriez me dire comment on pourra inviter les autres.

M. Beatty: C'est bien.

Le président: Est-ce que cela vous convient?

Le Barreau viendra témoigner et d'autres aussi, mais pour clarifier la question, il nous faut rencontrer ceux qui sont trempés dans ce secteur, je crois que ce sera un bon départ que de faire comparaître les représentants du ministère de la Justice, de la G.R.C. et de l'Association canadienne des fabricants d'équipement de bureau, sans compter les autres . . . En effet, il y a deux professeurs de l'université Western Ontario. Je ne les considère pas vraiment comme des témoins cependant; on pourrait quand même inviter l'un ou l'autre, ou les deux à la fois.

M. Robinson (Etobicoke—Lakeshore): Pouvez-vous nous dire quand nous devons présenter nos conclusions et nos recommandations? En deuxième lieu, notre Comité poursuivra-t-il ses travaux pendant la prochaine session, ou faudra-t-il que nous obtenions un mandat spécial pour demeurer en fonction? Je mentionne cela car il est certain que nous ne pourrions jamais entendre tous ces témoins d'ici là.

Le président: Cela dépend entièrement de votre recommandation. Pour ma part, j'ai l'impression qu'une fois notre calendrier établi et que nous aurons entendu des témoins le 30 mars, il ne nous restera qu'à tenir le comité principal au courant de ce que nous faisons, et de lui demander une prolongation tout en attendant de savoir où nous allons. Je n'ai pas d'idée sur la date de la fin de la présente session. En conséquence, s'il nous faut continuer à étudier la question au cours de la prochaine session, nous y réfléchirons lorsqu'elle commencera, mais pour le moment, je me contente de proposer que nous travaillions de façon ordonnée afin d'abattre le plus de besogne possible d'ici le 30 mars; après cela, si besoin est, nous poursuivrons nos travaux et demanderons au Comité de prolonger notre mandat.

M. Robinson (Etobicoke—Lakeshore): Avez-vous cependant l'intention de faire un rapport avant la fin de la session?

[Text]

Mr. Beatty: We have to give a progress report

The Chairman: A progress report, but I do not know so far when the end of the session will be, so if the session ends on June 30, of course we can have a report; it all depends, you know, if we are just having a budget and the session starts later on in the year. So I think we should proceed with inviting the three witnesses I mentioned.

Mr. Robinson (Etobicoke—Lakeshore): All right.

The Chairman: The next meeting will be 3:30 p.m. Thursday with the Justice department people.

Mr. Beatty: I have to speak at a meeting at 4:30 at one of the hotels in town here on Thursday, but at least I will be able to get an hour in if we get right underway. Thank you.

The Chairman: Okay.

The meeting is adjourned to the call of the Chair.

Thursday, March 17, 1983

• 1305

Le président: À l'ordre!

La séance peut débuter. Nos témoins, aujourd'hui, sont les fonctionnaires experts du ministère de la Justice. Je demanderai à M. Norman Hill de nous présenter les gens qui l'accompagnent afin que l'on puisse avoir, de la part des experts, un exposé sur la problématique qui confronte ce Comité.

Alors, monsieur Hill, je vous cède la parole.

Mr. Norman Hill (Project Chief, Theft and Fraud Project, Department of Justice): Thank you, Madam Chairman, and members of the subcommittee. The officials from the Department of Justice present are: Ms Elizabeth Gilhooly of the Criminal Law Review Section of the Department of Justice; Mr. Donald Piragoff, of the Criminal Law Amendment and Policy Planning Section of the Department of Justice; and Mr. Neville Avison, Chief of the Research and Statistics Section of the department.

• 1510

Madam Chairman, the Department of Justice is pleased to be able to assist the standing committee. We hope to be able to extend the same level of co-operation to you and to members as we did to the Hon. Perrin Beatty last year while he was developing the proposals he has now tabled in Parliament as Bill C-667.

I would like to indicate the division of responsibility for addressing the problems amongst the officials present. I will seek to assist you with reference to the process by which the department hopes to provide solutions to the problem that confronts the committee, and some of the strategies and reasons for adopting that process. I will seek to assist you in

[Translation]

M. Beatty: Nous devons faire un rapport provisoire.

Le président: Un rapport sur l'état des travaux, mais étant donné que je ne sais pas quand la session va prendre fin, tout ce que je puis dire, c'est que ce sera certainement possible de préparer un rapport si la session ne se terminera que le 30 juin. Cela dépend de toutes sortes de choses, vous savez, comme de la présentation d'un budget et de la mise en marche d'une nouvelle session plus tard cette année. Je suis donc d'avis que nous devrions commencer par inviter les trois témoins que j'ai mentionnés.

M. Robinson (Etobicoke—Lakeshore): C'est bien.

Le président: La prochaine réunion aura lieu à 15h30 jeudi, et nous entendrons les représentants du ministère de la Justice.

M. Beatty: Je dois prendre la parole lors d'une réunion qui se tiendra à 16h30, dans l'un des hôtels d'Ottawa jeudi, mais si nous commençons à temps, je pourrai participer pour au moins une heure. Merci.

Le président: C'est bien.

La séance est levée jusqu'à nouvelle convocation.

Le jeudi 17 mars 1983

The Chairman: Order please!

I call the meeting to order. We are receiving today expert witnesses from the Department of Justice. I would like to ask Mr. Norman Hill to introduce his colleagues. Our expert witnesses will brief us today on the general aspect of computer crime.

Mr. Hill, you now have the floor.

M. Norman Hill (chef de projet, Projet vol et fraude, ministère de la Justice): Merci, madame le président, membres du Sous-comité. Permettez-moi de vous présenter les fonctionnaires du ministère de la Justice: M^{me} Elizabeth Gilhooly du Service de révision du droit pénal du ministère de la Justice; M. Donald Piragoff, Section de l'élaboration de la politique et des modifications au droit pénal du ministère de la Justice et enfin M. Neville Avison, chef du Service de la recherche et des statistiques du ministère.

Madame le président, le ministère de la Justice a le plaisir de pouvoir aider le comité. Nous espérons établir les mêmes liens de collaboration avec les membres du comité que ceux que nous avons établis avec l'honorable Perrin Beatty l'année dernière alors qu'il élaborait le projet de loi déposé en Chambre, le projet de loi C-667.

J'aimerais vous informer de la division des responsabilités entre les fonctionnaires ici présents. Je verrai à vous conseiller sur les moyens envisagés par le ministère pour régler ce problème sur lequel se penche le comité; je vous expliquerai les stratégies et les justifications des recommandations présentées. Je vous aiderai à identifier les problèmes les plus complexes. Je

[Texte]

the identification of some of the more controversial and difficult issues that require solution. I will inform you of the consultations we have had to date and give a general description of our appreciation of the American experience and its relevance to Canada.

Mr. Piragoff will assist you on the problems arising from the state of the present law. He will deal specifically, in a general way, with certain proposals regarding the integrity of computer systems and he will touch upon some of the problems relating to the information issue, which is perhaps one of the most difficult ones in this complex area.

Mr. Avison will be able to assist you on any of the technical aspects of the problem on which you might wish to have some assistance. He will be able to give some idea of the techniques of computer abuse and he will also indicate the department's efforts to establish a data base so that we might be able to inform ourselves more fully on the nature and extent of the problem.

Ms Gilhooly will be providing the committee with a summary of the legislation in place in the United States, which contains the criminal sanctions relating to computer abuse.

Madam Chairman, the Department of Justice has, since the decision of the Supreme Court in the McLaughlin case, been seeking to provide some responses to this problem. However, those responses were directed to ad hoc amendments to the Criminal Code, which might be described more in the nature of closing loopholes.

For many reasons, some of which relate to happenings in the parliamentary process—on some occasions elections, on others difficulties in finding parliamentary time—none of those measures were ever tabled in Parliament. At the same time, the federal government was considering a complete overhaul of the Criminal Code and that process also gained momentum at the same time as when the other difficulties of which I spoke were in existence.

I think the Hon. Jean Chrétien, when he was Minister of Justice, announced that the federal government would be undertaking a comprehensive review of the criminal law. As a result of that decision by the federal government, certain projects were directed to the criminal law review section of the department. Amongst those projects were the principles and objectives of the criminal law and, secondly, theft and fraud, the revision of those provisions of the Criminal Code; I think they are Parts VII and VIII.

• 1515

The project team, of which Ms Gilhooly and I from part of the theft and fraud project, appreciated that some of the issues dealing with computer boosts had not been dealt with by the Low Reform Commission of Canada. During the course of last year the project team, comprised of myself, Ms Gilhooly and Mr. Piragoff, was established and given a mandate to consider the proposals which were in place for implementation through the criminal law amendment bills which had been developed from time to time, as well as a review of what would be

[Traduction]

vous relaterai les consultations que nous avons eues jusqu'à maintenant et enfin, je donnerai l'opinion générale du ministère sur ce qui s'est passé aux États-Unis et sur la pertinence de cette expérience au problème canadien.

M. Piragoff exposera les problèmes découlant de la loi actuelle. Plus précisément, il exposera certaines propositions sur le caractère inviolable des systèmes informatiques; il pourra aborder certains problèmes de l'aspect «information», un aspect des plus complexes.

M. Avison sera en mesure de vous expliquer les points techniques du problème. Il vous expliquera, d'une façon générale, les techniques de manipulation frauduleuse des ordinateurs, et il présentera ce qu'a fait le ministère pour se donner une base de données nous permettant de mieux nous informer sur la nature et l'étendue du problème.

M^{me} Gilhooly résumera à l'intention du comité les lois adoptées aux États-Unis, lois prévoyant des sanctions criminelles dans les cas d'infractions informatiques.

Madame le président, depuis le jugement de la Cour suprême dans l'affaire McLaughlin, le ministère de la Justice a cherché à résoudre ce problème. Cependant, les tentatives du ministère ont plutôt porté sur des modifications ponctuelles du Code criminel; en fait, le ministère a cherché à fermer les échappatoires.

Pour de nombreuses raisons, dont certaines ont trait au processus parlementaire, je pense ici aux élections et au manque de temps pour débattre des projets de loi, aucune de ces mesures ne fut présentée en Chambre. Parallèlement, le gouvernement fédéral envisageait une réforme globale du Code criminel. Cette réforme a vraiment été entreprise au moment où les problèmes d'infraction informatique commençaient à faire jour.

Si j'ai bonne mémoire, l'honorable Jean Chrétien, alors qu'il était ministre de la Justice, a déclaré que le gouvernement fédéral avait l'intention d'entreprendre une réforme globale du droit criminel. Après cette décision du gouvernement fédéral, le Service de révision du droit pénal du Ministère a été chargé de certains projets. On compte notamment le projet d'étude des principes et des objectifs du droit pénal et également le Projet vol et fraude prévoyant certaines révisions du Code criminel aux parties, je crois, VII et VIII.

L'équipe du projet fraude et vol, dont M^{me} Gilhooly et moi-même faisons partie, s'est rendu compte que certains aspects des crimes informatiques n'avaient pas été touchés par la Commission de réforme du droit du Canada. L'année dernière, l'équipe a été formée de moi-même, de M^{me} Gilhooly et de M. Piragoff; nous devons étudier les propositions envisagées aux différents projets de loi portant modification du Code criminel et nous devons également entreprendre une étude des mesures nécessaires pour régler ce problème de façon logique et globale.

[Text]

required to deal with the problem in a comprehensive and integrated way.

So I would like to turn, first of all, to the terms of reference of the Computer Crime Project within the Department of Justice. There are two aspects to our terms of reference. The first relates to a review of the proposals to amend the Criminal Code in relation to the unauthorized use of computers and the destruction or alteration of the information stored therein. The second is to conduct a study of existing and future technological advances in the computer and telecommunication industries, the security problems associated with these advances, and to determine the need for further legislative action from both a civil and criminal point of view.

Madam Chairman, we have tabled with the committee a number of documents. I would just like to refer to the first one, and I apologize for the fact that we were not able to have it in both official languages.

The first document is an outline of the department's proposals for safe-guarding computer systems. That document essentially identifies five errors of wrongful conduct or problems in relation to the integrative computer systems not now adequately covered by the criminal law. To the right of it, we indicate six possible solutions. The fourth has an alternative. Mr. Piragoff will develop the rationale and the effect these proposals would have on the existing provisions in the Criminal Code.

I would just like to indicate, Madam Chairman, that at the present time these proposals are in an advanced state of preparation for legislative action, should the Minister of Justice so desire and should parliamentary time be available.

• 1520

Now, given the complex nature of the effect and the role of computer technology in society as a whole, it is necessary to educate ourselves about the nature and extent of the problem, to identify examples of actual abuse, mechanisms to prevent, avoid, and deter abuse; to identify the adequacy or assess the adequacy of those mechanisms, and to determine the need for additional mechanisms, or solutions, legislative or otherwise. Our initial efforts were directed to a review of the literature relating to the problem, to learning about the experience in other jurisdictions, in particular the United States, to identifying the issues and problems, and to undertaking the widest possible consultations with experts, inside and outside Canada, on different aspects of computer abuse.

I emphasize this because there is some basis for suggesting that the department has been taking some time in coming up with solutions. I would like to dispel the notion that our work is a reflection of a lack of interest. Rather, it is more in keeping with the desire to produce a worthwhile product. We acknowledge that technological advances in computer applications have produced major benefits to society, and that computers have introduced innovations into the business world, the communications media, and the educational and scientific community. In addition, as computers have developed, new methods of perpetrating crime have emerged.

[Translation]

J'aimerais tout d'abord vous donner le mandat du Projet sur les crimes informatiques du ministère de la Justice. Notre mandat est double. Tout d'abord, nous devons étudier les propositions de modification du Code criminel en ce qu'elles ont trait à l'utilisation non autorisée des ordinateurs et à la destruction ou à la falsification des informations qui sont en mémoire dans l'ordinateur. Nous devons parallèlement mener une étude des progrès technologiques à venir dans le domaine de l'informatique et des télécommunications, nous devons cerner les problèmes de sécurité qui en découlent et déterminer s'il y a lieu d'adopter des mesures législatives civiles ou criminelles.

Madame le président, nous avons déposé certains documents auprès du Comité. J'aimerais ici faire référence au premier document, lequel, je m'en excuse, n'est pas disponible encore dans les deux langues officielles.

Ce document décrit les mesures envisagées par le Ministère pour assurer la sécurité informatique et décrit les cinq erreurs ou problèmes d'utilisation des ordinateurs intégrés, problèmes qui ne sont pas prévus dans le droit criminel. Sur le côté droit de la feuille, nous donnons six possibilités de solution. Il y a deux façons de résoudre le quatrième problème. M. Piragoff expliquera les répercussions de ces propositions sur les dispositions actuelles du Code criminel.

J'aimerais dire ici, madame le président, qu'à l'heure actuelle, ces propositions sont à toutes fins utiles prêtes à être présentées en Chambre, si le ministre de la Justice le désire, et si la Chambre a le temps nécessaire pour les étudier.

Étant donné la complexité de la science informatique et du rôle que jouent les ordinateurs dans notre société, nous devons nous renseigner sur la nature et la portée du problème, nous devons identifier des exemples de manipulations frauduleuses, ainsi que les mécanismes de protection nécessaires; nous devons juger de la pertinence de ces mécanismes et voir s'il n'y aurait pas lieu d'adopter d'autres mesures législatives ou autres. Nous avons tout d'abord entrepris d'étudier la documentation sur ce problème afin de voir ce qui a été fait à l'étranger, notamment aux États-Unis, d'identifier les problèmes et d'entreprendre les consultations les plus complètes possibles avec des spécialistes canadiens et étrangers au sujet des manipulations frauduleuses des ordinateurs.

J'insiste là-dessus car certains ont fait valoir que le ministère s'était traîné les pieds avant de présenter des solutions. Cette lenteur apparente n'indique pas un manque d'intérêt, au contraire, elle démontre plutôt que nous voulons présenter des solutions qui se tiennent. Nous reconnaissons que les progrès technologiques en matière informatique ont grandement profité à l'ensemble de la société; les ordinateurs ont été des plus utiles dans les mondes des affaires, des communications, de l'enseignement et de la recherche scientifique. Cependant, à mesure que la science informatique avançait, de nouvelles méthodes criminelles étaient créées.

[Texte]

I think we can identify three parts to the problem. The first is the unauthorized acquisition or destruction of the hardware; for example, the actual machines, tapes, and printouts. The second is the unauthorized acquisition or destruction of data stored therein; and thirdly, the unauthorized use of computer services.

The first, which concerns tangible items, is already covered by the general provisions of the Criminal Code concerning theft and mischief. Against this background there were two existing factors which determined the strategy for dealing with this problem. The first insofar as criminal sanctions were concerned was the statement of principles of the purpose of the criminal law formulated by the government as a guide for the reform of the criminal law. This had to be kept uppermost in our work. Briefly, the purpose of the criminal law is to contribute to the maintenance of a just, peaceful, and safe society through the establishment of a system of prohibitions, sanctions, and procedures, to deal fairly and appropriately, with culpable conduct that causes or threatens serious harm to individuals or society.

The second was that if it was possible to do so, any new criminal sanctions ought to be part of the existing framework of our present criminal law. The advantages of this approach seem to outweigh any disadvantages that may be identified. For example, there is the existing familiarity with the principles of the current criminal law of judges, lawyers, and law enforcement officials. This is not to say that we may not be facing a challenge to develop new concepts to deal with the larger issue of information in general.

One of the first problems we faced, Madam Chairman, was the difficulty in obtaining data on the incidence of computer abuse and crimes committed with the use of computers inside Canada. This data would bring into focus the types of conduct which criminal sanctions should address.

• 1525

It was our view that criminal sanctions should be directed to the method or conduct involved in computer abuse and crimes associated with the use of computers, if one is to avoid the laws' being outdated as a result of the new technology. In other words, we felt the conduct is what we should be looking at rather than the technology.

We also felt it was important to determine what types of conduct ought to be the subject of criminal sanctions in order to establish a realistic basis for determining these types of conducts. Through the assistance of Mr. Don Parker, an expert in the area of computer abuse of Stanford Research Institute International, the project team obtained the data base of Mr. Parker and reviewed nearly 1,000 cases, including 10 Canadian cases, which appeared from his files and which had occurred during the years 1966 to 1982. We felt this was important because of the fact that there was little, if any, data available to us in Canada.

Our major concern in this exercise was to ensure that any legislative scheme the federal government proposed would

[Traduction]

Le problème, selon moi, se divise en trois catégories. Tout d'abord, il y a l'acquisition ou la destruction non autorisée du matériel, par exemple, les unités de traitement, les bandes magnétiques et les imprimés. En deuxième catégorie, nous donnons l'acquisition ou la destruction non autorisée des données qui sont dans la mémoire de l'ordinateur; troisièmement, nous avons l'utilisation non autorisée des services informatiques.

La première catégorie, portant sur des biens matériels, est déjà prévue aux dispositions générales du Code criminel portant sur le vol et les méfaits. Dans ce contexte, deux facteurs ont déterminé notre stratégie. Tout d'abord, au sujet des sanctions criminelles, le gouvernement, dans sa déclaration d'intention de réforme du Droit criminel, avait stipulé certains principes généraux. Ces principes devaient nous guider tout au long de notre travail. Pour résumer, le gouvernement avait déclaré que le droit criminel doit contribuer à assurer une société juste, pacifique et sécuritaire en adoptant un système d'interdictions, de sanctions et de formalités permettant de traiter équitablement les actes répréhensibles qui menacent les personnes ou la société.

Deuxième facteur: nous devons dans la mesure du possible intégrer toute nouvelle sanction criminelle dans le cadre existant du droit criminel. Cette approche présente plus d'avantages que d'inconvénients. Par exemple, les juges, les avocats et les services de police connaissent déjà les principes du droit criminel. Cela ne signifie pas que nous n'aurons pas éventuellement à élaborer de nouveaux principes dans ce domaine général de l'information.

Dans le cadre de notre étude, un problème a émergé très rapidement. Nous avons eu de la difficulté à obtenir des données sur les fraudes et crimes informatiques au Canada. Ces données devaient nous permettre de cerner les méfaits pour lesquels des sanctions criminelles devraient être prévues.

Nous avons pensé que des sanctions criminelles devraient condamner la méthode ou le comportement des fraudeurs de l'informatique pour ne pas que les lois soient dépassées par les progrès technologiques. Autrement dit, il faut se pencher sur le comportement plutôt que sur la technologie.

Nous avons également pensé qu'il fallait cerner les types de comportements qui devraient être condamnés par des sanctions criminelles. Grâce à la collaboration de M. Don Parker, un spécialiste du *Stanford Research Institute International* dans le domaine de la fraude informatique, l'équipe de projet a pu obtenir la base de données de M. Parker; nous avons étudié près de 1,000 cas, dont dix sont survenus au Canada, qui s'étaient produits entre 1966 et 1982. Nous avons choisi de procéder de cette façon parce qu'il n'y avait que très peu de données pour le Canada.

Dans cette partie de notre étude, nous avons voulu faire en sorte que les mesures législatives que présenterait le gouverne-

[Text]

cover all the known types of abuse, which it was felt should be the subject of criminal sanctions. In other words, we did not want to create a scheme which omitted certain types of conducts or created loopholes so people would be able to legitimately argue that Parliament did not intend to include those types of conduct.

Apart from the question of the unauthorized acquisition, use and disclosure of information, we are satisfied that the legislative scheme proposed—which is in the document to which I referred earlier and with which Mr. Piragoff will deal—would encompass all those types of conduct which might be the subject of criminal sanctions. So apart from the information questions, which will be addressed quite separately in our project, we would be happy to discover whether or not we are accurate in our assessment.

During the course of our consultations, we have obtained the results of surveys done inside and outside Canada. I would just like to refer briefly to one of the surveys conducted by the Ontario Provincial Police because I believe it is important that members of the committee appreciate the reality in terms of the statistics.

In November of 1980, the Ontario Provincial Police mailed a survey on computer crime and security to the Ontario offices of 640 corporations and institutions. As of June 1, 1981, 321 responses were received. Some of the results of this survey are of interest. I am not dealing with the results of the entire survey; I just want to focus on one aspect of it.

Only 13 companies reported experiencing a loss through computer abuse. The incidents reported can be summarized as follows. First, theft of computer processing time and malicious damage to files or hardware combine equally to form two-thirds of the reported cases. Second, the remaining one-third involved misappropriation of programs and data, abuse of a computerized cash-dispensing machine, processing of false invoices through the system; and in one instance, the reported abuse related to an employee's giving false credentials about his computer expertise.

Only five of the 13 incidents were reported to the police, and only three prosecutions appear to have been undertaken. One was withdrawn; one conviction was registered, believed to be malicious damage, and the third is still before the courts.

• 1530

What conclusions does this small number of reported cases lead to? Is it that there are few cases of computer abuse or is it that victims are reluctant to report incidents of computer abuse and view alternative means of dealing with it, or is it a combination of both? Whatever the true answer is, it is clear that there is a great potential for harm in some types of computer abuse. Among the documents which we have tabled in a binder, which has been handed out through the club, is a

[Translation]

ment couvrent tous les types connus de fraudes qui devraient faire l'objet de sanctions criminelles. Autrement dit, nous n'avons pas voulu mettre en place un régime qui aurait omis certains types de comportement ou qui aurait créé des échappatoires permettant aux juristes de faire valoir que le Parlement n'avait pas l'intention d'inclure ces types de comportements.

Mise à part la question de l'acquisition, de l'utilisation et de la divulgation non autorisée des données, nous sommes convaincus que les mesures législatives envisagées, lesquelles sont énumérées dans le document auquel j'ai fait référence précédemment et seront expliquées par M. Piragoff, prévoiront tous les types de comportements qu'il conviendrait de condamner par des sanctions criminelles. Donc, mises à part les questions portant sur l'information, qui feront l'objet d'une sous-étude distincte, nous sommes prêts à voir si, de fait, notre opinion est juste.

Au cours de nos consultations, nous avons reçu les résultats d'enquêtes effectués au Canada et à l'étranger. J'aimerais ici vous présenter rapidement une de ces enquêtes menée par la police provinciale de l'Ontario; les membres du sous-comité doivent, selon moi, avoir une bonne idée des statistiques dans ce domaine.

En novembre 1980, la police provinciale de l'Ontario a envoyé une enquête portant sur les crimes et la sécurité informatique à quelque 640 sociétés commerciales et institutions ayant des bureaux en Ontario. Au 1^{er} juin 1981, 321 questionnaires avaient été retournés. Certains résultats de cette enquête sont intéressants; je ne donnerai pas les résultats de l'ensemble de l'enquête, mais je vais plutôt en expliquer un aspect.

Seulement treize sociétés ont déclaré avoir eu des pertes dues à des fraudes informatiques. On peut catégoriser les incidents. Tout d'abord, le vol de temps-machine et les dommages volontaires aux dossiers ou au matériel représente les deux-tiers des cas signalés. Les autres cas portent sur le détournement de programmes et de données, la manipulation de guichets automatiques, le traitement de comptes inventés dans l'ordinateur. Dans un cas, la manipulation signalée portait sur un employé ayant modifié son expérience et ses compétences en matière d'informatique.

La police n'a été saisie que de cinq des 13 incidents et il semblerait que seulement trois causes ont été portées en justice. Une de ces causes a été retirée, une condamnation a été enregistrée, il semble que c'était une question de dommages causés avec intention de nuire. La troisième affaire est toujours devant les tribunaux.

Quelles conclusions peut-on tirer de ce petit nombre de cas déclarés? Cela veut-il dire qu'il y ait très peu de cas de fraude relative aux ordinateurs ou encore, que les victimes hésitent à signaler ce genre de cas ou préfèrent utiliser d'autres moyens pour obtenir réparation, ou encore une combinaison des deux? Quelle que soit la réponse, il n'en demeure pas moins que certains genres de fraude relative aux ordinateurs présentent un grand potentiel de dommage. Vous trouverez dans le

[Texte]

very interesting article, Madam Chairman, by Mr. Peter Watkins in a Canadian magazine. It is entitled: "Computer Crime, Myth from the Reality". I will not read through it but I would just simply commend it to the members of the committee in terms of his approach to dealing with the statistics.

Clearly there is a problem with regard to reporting, and in this regard one of the first issues that of course law enforcement officials are concerned about is, is whether it is possible to encourage reporting through some mandatory reporting requirement or, alternatively, should we devise a legislative scheme which encourages the reporting of incidences which may result in more prosecutions.

At least three states in the United States have mandatory reporting requirements. Unfortunately, so far we have been unable to obtain any data with respect to the impact of those provisions on the rate of prosecutions in those three states.

I would like now to turn to deal with the protection of information in general, apart from the issue of abuse of computer systems.

Perhaps the most important aspect of the complex problem which faces the committee is how to come to terms with the question of the unauthorized acquisition, use and disclosure of information. One approach has been suggested by Mr. Beatty in his bill. However, it is the department's view that this matter is so complex that it ought to be carefully studied, and in this regard I would like to highlight some of the problems which I am sure the committee will be confronted with during the course of their consideration of the subject matter.

The two critical changes in our view are, first, the ability to devise new legal, economic and social arrangements that will ensure the creation and the effective and profitable utilization of new information and technology.

The second challenges a liberal society to protect its basic political and human values from unwise application, withdrawals or restrictions of that new knowledge.

The fundamental issue is whether all information should be treated as a proprietary commodity or as a resource in society or, if it should be treated as both, the circumstances in which emphasis should be placed on one aspect or the other.

• 1535

Alternatively, should some information be treated as a proprietary commodity, and which information should be accorded that status; and, if so, should it be the criminal law,

[Traduction]

classeur que nous vous avons fait remettre par le greffier un article fort intéressant que M. Peter Watkins a publié dans une revue canadienne. Cet article s'intitule: *Computer Crime, Myth from the Reality* (Les infractions relatives aux ordinateurs, la différence entre le mythe et la réalité). Je ne vais pas le lire, mais je recommande vivement aux membres du Comité d'en prendre connaissance, car l'approche qu'utilise l'auteur à l'égard des statistiques est des plus intéressante.

Nous faisons manifestement face à un problème de divulgation. L'une des grandes questions qui se pose par conséquent aux responsables de l'application de la Loi consiste à déterminer s'il est possible d'encourager les victimes de ce genre d'infractions à les signaler en adoptant des exigences en ce sens ou alors, en mettant au point des mesures législatives susceptibles, éventuellement, d'entraîner un plus grand nombre de poursuites.

Au moins trois États américains ont adopté des dispositions législatives qui exigent des victimes d'infractions relatives aux ordinateurs de les signaler aux autorités compétentes. Malheureusement, nous n'avons pas pu jusqu'à maintenant obtenir de données sur l'incidence que ces dispositions ont eue sur le taux de poursuite dans ces trois États.

J'aimerais maintenant passer à la question de la protection de l'information en général, sans traiter du problème des fraudes relatives aux ordinateurs.

Je pense que l'aspect le plus important du problème fort complexe dont est saisi ce Comité, c'est la façon d'aborder le problème de l'acquisition, de l'utilisation et de la divulgation non autorisées de l'information. M. Beatty propose une approche dans son projet de loi. Cependant, le ministère est d'avis que le problème est tellement complexe qu'il nécessite une étude approfondie. Je vais vous donner un aperçu de certains des problèmes que le Comité sera certainement appelé à aborder dans le cadre de son examen de la situation.

A notre avis, deux changements de base s'imposent, à savoir, la capacité de mettre au point de nouveaux arrangements juridiques, économiques et sociaux, qui garantiront la création et l'usage efficace et rentable de nouvelles données et de nouveaux processus technologiques.

Le deuxième défi qui se pose à la société libérale est de trouver le moyen de protéger ses valeurs de base tant politiques qu'humaines contre tout usage mal avisé, tout retrait ou toute restriction des nouvelles connaissances.

La question fondamentale qui se pose consiste donc à déterminer si toute information doit être considérée comme un bien privé ou comme une ressource de la société. En outre, si l'on arrive à la conclusion que ces deux définitions s'appliquent ensemble à l'information, il faudra déterminer les circonstances dans lesquelles il convient de mettre l'accent sur l'un de ces aspects par opposition à l'autre.

Il faudra aussi déterminer si certaines catégories de données devront être considérées comme un bien privé et, dans l'affirmative, les catégories qui rentreront dans cette définition. De plus, il faudra décider si cette définition sera incluse dans le

[Text]

the statutory monopolies or the civil law that accords that status, or one or another or all of them?

We are approaching the problem of information not simply from the point of view of information in computers because we do not think that is the total picture. It is interesting to note that presently in Canada some 53 statutes contain prohibitions against disclosures of information so insofar as those particular statutes are concerned there are sanctions in place dealing with that group or class of information.

Madam Chairman, in order to facilitate the consultation process on this subject a background paper identifying the issues related to the abuse of computer systems was prepared and circulated. Attached to that background paper is an article by R. Grant Hammond, counsel to the Alberta Institute of Law Research and Reform. That document has been tabled and is in the binder we have submitted to the clerk.

In that document we focus on some of the problems associated with information as well as some of the other issues which arise for consideration. Professor Hammond addresses a number of legal and socio-economic issues relating to the ascription of proprietary rights to information, the role of information in the post-industrial society, judicial responses to information questions and the need to develop new legal paradigms in respect of information. We have tabled these documents for the consideration of the committee.

In his presentation in Parliament, Mr. MacBain, the Parliamentary Secretary to the Minister of Justice, highlighted some of the conceptual difficulties raised by the approach adopted by Mr. Beatty in his bill, and we would, without wishing to repeat all that he said, like to commend some of his comments and the examples given to the committee for careful consideration.

In particular, we share the view that the institution of property may be an appropriate vehicle for dealing with some aspects of information; however, it is difficult to conceive that all information in a computer could be property. Some of it may be knowledge that is already public and known and possessed by many in their own minds. Should it automatically become someone's property merely because he puts it into his computer? Why is it not property when it is in my head or in my filing cabinet? How can it be property and thereby give the owner of the computer the exclusive right to possess it if the information is also possessed in the minds of half the population of Canada? What if someone else independently creates the same information? Can it be said that this person has no right to possess or to use the information he created? There are many other examples which appear in Mr. MacBain's presentation.

I would also like to refer to some points raised during one of our consultations which I think are very important with regard to information.

[Translation]

droit criminel, les dispositions relatives aux monopoles légaux d'exploitation, ou le droit civil, ou encore, dans deux de ces textes législatifs ou les trois en même temps.

Notre approche à l'information ne se limite pas aux données informatisées parce que ces dernières, à notre avis, ne constituent qu'un des éléments du problème. Il est intéressant de constater que quelque 53 lois canadiennes comprennent à l'heure actuelle des dispositions d'interdiction contre la divulgation de l'information et il existe donc des sanctions relatives à ce groupe ou à cette catégorie d'information.

Madame le président, un document d'information concernant les divers aspects des fraudes relatives aux ordinateurs a été rédigé et distribué dans le but de faciliter le processus de consultation sur cette question. Vous trouverez annexé à ce document d'information un article de R. Grant Hammond, conseiller juridique auprès de l'*Alberta Institute of Law Research and Reform*. Ce document se trouve dans la liasse que nous avons remise au greffier.

Ce document traite de certains des problèmes liés à l'information ainsi que d'autres sujets d'étude. M. Hammond se penche dans son article sur certains des problèmes juridiques et socio-économiques relatifs à la reconnaissance des droits de propriété dans le domaine de l'information, au rôle de l'information dans la société post-industrielle, aux réponses juridiques aux questions d'information et à la nécessité de mettre au point de nouveaux modèles juridiques dans ce domaine. Nous avons remis ce document pour la considération du Comité.

Dans un exposé qu'il a fait au Parlement, M. MacBain, le secrétaire parlementaire du ministre de la Justice, a souligné certaines des difficultés théoriques qui découlent de l'approche que M. Beatty a adoptée dans son projet de loi et, sans vouloir répéter tout ce qu'il a dit, nous recommandons aux membres du Comité d'accorder une attention particulière à ses observations et à ses exemples.

Nous partageons en particulier son avis sur le fait que l'institution de la propriété pourrait être un moyen approprié de traiter certains aspects de l'information. Cependant, il est difficile d'accepter que toutes les données informatisées pourraient être considérées comme un bien privé. En effet, certains de ces éléments de connaissance sont déjà publics et connus de nombreuses personnes. Le fait qu'une personne verse une donnée dans son ordinateur suffit-il pour que cette donnée devienne sa propriété? Pourquoi alors une donnée ne serait-elle pas ma propriété si je l'ai en tête ou dans mes dossiers? Comment une donnée peut-elle être considérée comme un bien privé et comment est-ce que le propriétaire d'un ordinateur peut-il jouir du droit exclusif de posséder une donnée si elle est déjà connue de la moitié de la population du Canada? Que se passerait-il si quelqu'un d'autre arrive indépendamment à la même information? Pourrait-on dire à ce moment-là que cette personne n'a pas le droit de posséder ou d'utiliser une donnée d'information qu'elle a créée? M. MacBain donne Beaucoup d'autres exemples dans son exposé.

J'aimerais également vous parler de certains points qui ont été soulevés dans le cadre d'une de nos séances de consultation car, à mon avis, ils revêtent une importance toute particulière dans le contexte de l'information.

[Texte]

• 1540

They suggested that in terms of property rights and information it might be dangerous to use the Criminal Code to create property rights which do not exist in civil law. Bearing in mind the statutory monopoly scheme in the copyright law, which has a limitation of 50 years—which would expire 50 years after the death of the author—it would not be an offence under the copyright law to copy something at that time. However, if the Criminal Code provision were used, then it would be in the nature of an apparent conflict.

It would also be considered dangerous if perpetual property protection were used in situations which are already covered by the statutory monopoly of copyright. And of course, bearing in mind access to information provisions, problems could arise in the protection of property based on the desire to provide access after a certain time.

So it was our view that a comprehensive study should be undertaken on this complex issue; and to that end we asked Professor Hammond to undertake a study on all the various aspects of dealing with information, in both its criminal and its civil aspects. The Alberta Institute of Law Research and Reform was also interested in this topic, obviously because there is a provincial interest in certain aspects of information and the proprietary rights of certain types of information. We hope that report will be ready by the spring, and when that report has been completed, then consultations will begin on this aspect of the problem.

A brief review of some of the matters which Professor Hammond will be looking at might be in order, as we have provided Professor Hammond's name as a possible witness to assist the committee. He will be looking at the jurisprudential problems arising out of the use of the criminal sanction; for example, the concept of deprivation and exportation, the problem of evaluation of information, the differences between the civil law descriptions of property rights to some types of information, and some of the alternative ways of avoiding some of the problems of ascribing proprietary rights to information, which may involve developing new and flexible legal structures to maintain the balance which has to be maintained between the free flow of information on the one hand and the need to provide an incentive for people to innovate and to create new ideas and new technology.

He will be looking at the civil law protection in place in both the federal and the provincial jurisdictions, and he will be assessing the adequacy of civil law protection. At the present time there exist three broad categories of civil law protection: the federal protection through the statutory monopolies, if they may be described as "civil" for the time being; that is, the copyright, trademark and patent. Then there is the provincial common law through contract, tort, and some of the common

[Traduction]

En effet, certains ont prétendu qu'il pourrait être dangereux d'intégrer au Code criminel des dispositions sur les droits de propriété en matière d'information qui n'existent pas dans le droit civil. Si l'on tient compte du fait que la Loi sur les droits d'auteur prévoit un monopole légal d'exploitation d'une limite de 50 ans—c'est-à-dire que le monopole expire 50 ans après le décès de l'auteur—cela veut dire que quiconque copie quelque chose à ce moment-là enfreint le droit d'auteur. Toutefois, si une disposition du Code criminel devait s'appliquer, cela serait susceptible de donner lieu à un conflit apparent.

Il pourrait également être dangereux d'appliquer des dispositions de protection de la propriété à perpétuité dans des situations que couvre déjà le monopole légal prévu dans le contexte des droits d'auteur. En outre, comme nous avons des dispositions législatives qui prévoient l'accès à l'information, la protection de la propriété pourrait poser des problèmes, surtout si l'on veut donner accès à l'information ainsi couverte après un certain laps de temps.

C'est pourquoi nous sommes arrivés à la conclusion qu'il convenait d'effectuer une étude exhaustive de cette question fort complexe. C'est la raison pour laquelle nous avons demandé à M. Hammond d'entreprendre une étude des divers aspects, tant criminels que civils de l'information. L'*Alberta Institute of Law Research and Reform* a manifesté de l'intérêt à cet égard, probablement parce que la province s'intéresse à certains aspects de l'information et les droits de propriété liés à un certain genre d'information. Nous espérons que ce rapport sera terminé d'ici le printemps. Une fois ce rapport terminé, nous pourrions entreprendre des consultations sur cet aspect du problème.

Un bref examen de certaines des questions sur lesquelles le professeur Hammond se penchera pourrait être utile et nous avons donc recommandé au Comité d'inviter M. Hammond à venir témoigner. Il étudiera les problèmes de jurisprudence qui découlent de l'application de sanctions criminelles, comme par exemple, le principe de la privation et de l'exportation, ainsi que le problème de l'évaluation de l'information, la différence entre la définition des droits de propriété eu égard à certains genres d'information dans le Droit civil, ainsi que certains moyens d'éviter les problèmes liés à la reconnaissance de droits de propriété à l'égard de certaines données d'information qui pourraient exiger la mise au point de nouvelles structures juridiques souples dans le but de maintenir l'équilibre nécessaire pour faciliter le libre échange de l'information, d'une part, et la nécessité d'encourager l'innovation et la création de nouvelles idées et de nouveaux processus technologiques d'autre part.

M. Hammond se penchera également sur les mesures de protection qui existent déjà dans le droit civil tant au niveau fédéral que provincial et déterminera si elles sont adéquates. À l'heure actuelle, il existe trois catégories générales de protection dans le Droit civil: la protection fédérale par l'application de monopoles légaux d'exploitation, en qualifiant ces derniers de recours civils pour les besoins de la cause. Ces dispositions comprennent trois éléments, à savoir, les droits d'auteur, les marques de commerce et les brevets. Il y a ensuite le droit

[Text]

law elements of property law and equity, which are directed mainly to providing relief in the area of trade secrets.

• 1545

Then there are some provincial statutes, for example, the privacy acts. And then finally he will consider whether, having analyzed all of the above, whether or not a multi-vehicle approach—that is, the use of a combination of criminal and civil sanctions—might not be the most appropriate response.

So having dealt with our strategy in relation to information through the use of Professor Hammond's expertise, I would like to turn briefly to the procedural and evidentiary problems which we have identified, and which are associated with the investigation and enforcement of computer abuse. I am sure that Superintendent Allen will expand on some of these from the point of view of the RCMP. However, purely from a point of view of indicating some of the problems we have identified, I would like just simply to enumerate them.

First is the problem of search: searches and search warrants. And it might be of interest to note that we have consulted with an assistant United States attorney who happened to have been able to obtain a search warrant to get into a computer successfully to obtain the fruits of the crime, which enabled him to initiate a prosecution. His view was that it largely depended on the drafting of the order which you wanted in relation to the particular establishment, the computer system.

The other one relates to evidence, and I think I would just like to make two comments here. The first is to state that in relation to the provisions of Mr. Beatty's bill which relate to amendments to the Canada Evidence Act, I would like to point out that there is a bill currently before the Legal and Constitutional Affairs Standing Senate Committee—I think it is S-33—a government measure which has a provision, Section 130, which in our judgment ameliorates the problem posed by Mr. Beatty.

The third procedural problem is that of jurisdiction. This is much more difficult because of the considerable trans-border data flow and electronic transfer of funds going between, for example, United States and Canada. More difficult because of the state of the technology, with remote terminals giving access across national boundaries. We are looking at the possibility of developing a proposal to establish an international convention which would treat computer crime in the same way that piracy is now treated in the international arena. I thought I would indicate that to members of the committee.

The fourth is extradition. The only comment I would make at this stage is that if we can find a legislative scheme which brings the new solutions within the existing framework of the criminal law, then we may be able to overcome the problem of

[Translation]

commun des provinces qui comprend des dispositions sur les contrats, les délits, ainsi que certains aspects du droit de la propriété et des avoirs, qui accordent des dédommagements dans le domaine des secrets de fabrication.

Il existe en outre des lois provinciales, par exemple sur la protection de la vie privée. Une fois que M. Hammond aura étudié tous ces aspects, il déterminera si une approche multivalente, à savoir, l'application d'une combinaison de sanctions criminelles et civiles, ne s'avérerait pas la mesure la plus efficace.

Maintenant que je vous ai décrit la stratégie que nous avons adoptée à l'égard de l'information en ayant recours aux compétences de M. Hammond, je vais vous expliquer brièvement les problèmes de procédure et de preuve que nous avons cernés dans le contexte des enquêtes sur les fraudes relatives aux ordinateurs et de l'application des textes législatifs pertinents. Je suis persuadé que le surintendant Allen s'étendra sur certains de ces problèmes du point de vue de la GRC. Cependant, je vais vous énumérer les problèmes que nous avons cernés.

Il y a d'abord le problème de la perquisition et des mandats de perquisition. Il vous sera utile d'apprendre que nous avons consulté un procureur adjoint des États-Unis qui a réussi à obtenir un mandat de perquisition lui donnant accès à un ordinateur, ce qui lui a permis d'obtenir une preuve sur les produits de cette infraction et, par le fait même, d'intenter des poursuites. Ce dernier était d'avis que le succès de ce genre d'entreprise dépendait de beaucoup de la formulation du mandat nécessaire pour obtenir accès à un établissement particulier et à son réseau d'ordinateurs.

J'aurais deux observations à faire pour ce qui concerne la preuve. Il convient, je crois, de signaler, eu égard aux dispositions du projet de loi de M. Beatty qui recommande des modifications à la Loi canadienne sur la preuve, que le Comité permanent du Sénat sur les questions juridiques et constitutionnelles est actuellement saisi d'un projet de loi—je crois qu'il s'agit du bill S-33—une initiative du gouvernement qui contient une disposition, l'article 130, qui, à notre avis, serait susceptible de régler le problème que pose M. Beatty.

Le troisième problème de procédure concerne la juridiction. C'est un problème beaucoup plus complexe en ce sens qu'il y a beaucoup d'échanges de données et de transferts de fonds internationaux comme par exemple, entre le Canada et les États-Unis. Ce problème est d'autant plus compliqué que l'avancement de la technologie permet l'échange de données à travers les frontières par l'utilisation de terminaux éloignés. Nous étudions actuellement la possibilité de mettre au point un projet de convention internationale qui traiterait les infractions relatives aux ordinateurs de la même façon que la piraterie à l'échelle internationale. J'ai pensé que cet élément d'information était susceptible d'intéresser les membres du Comité.

Le quatrième problème est celui de l'extradition. J'ai une seule observation à faire à cet égard maintenant. Si nous réussissons à trouver un moyen législatif susceptible d'offrir de nouvelles solutions à l'intérieur de la structure actuelle du droit

[Texte]

reciprocity of offences. That is, we may be able to use the existing offences in the respective extradition treaties to be able to effectively enforce offences. If new offences are created, then new agreements will have to be negotiated.

The fifth one relates to restitution and compensation, and in this regard I would just like to make two comments.

• 1550

The first is that it is clearly desirable that where large profits are obtained from computer abuse, these profits should be effectively be stripped from the wrongdoer. It may be problematic as to whether or not the current provisions of the Criminal Code would be able to do that, and that is another reason why careful consideration has to be given to the multi-vehicle approach so as to be able to provide proper compensation and restitution in appropriate cases. I would also like to point to the fact that in the United States a very effective means of stripping the profits from wrongdoers was introduced through the 1980 amendments to the U.S. Copyright Act

Finally, on the question of valuation, I would just like to indicate that we share the same concerns which are reflected in Mr. Beatty's presentation about this problem. I think that to some extent we may have found a solution with regard to the mischief provision insofar as it affects the jurisdiction of the court, and Mr. Piragoff will address that issue. However, in relation to the criminal sanctions, these are usually more important in relation to compensation, even more important in relation to civil remedies, to be able to have a realistic measure of compensation; more so than in the area of jurisdiction.

So the only comment on reporting requirements is that in the United States our consultations with a member of the FBI indicated that their push to have reporting requirements was largely predicated on this basis. Assuming for the moment that you are able to provide new laws, new sanctions: how would you evaluate those if having passed those laws there was no improvement in the rate of prosecution? Would it be a case of saying that the law was not necessary? Would it be a case of saying that people continue not to report? What is the basis for the change or the lack of change in that state of affairs? So that has been the significant reason advanced for having the mandatory reporting requirements.

Another important strategy which we adopted in dealing with our work was to attempt to co-ordinate all the federal initiatives which impacted on our problem. We identified these to be the new access to information laws, the privacy laws, the fact that there exists different classifications of types of information—for example, trade secrets, official secrets and

[Traduction]

criminel, nous réussissons peut-être à surmonter le problème du caractère réciproque des infractions. En d'autres termes, nous pourrions peut-être utiliser la définition actuelle d'infractions des traités d'extradition respectifs pour appliquer plus efficacement les lois qui les concernent. En effet, si nous créons de nouvelles infractions, il nous faudra alors négocier de nouvelles ententes.

Le cinquième problème porte sur la réparation et le redressement. J'ai deux seules observations à faire sur cet aspect.

Premièrement, nous estimons qu'il est tout à fait souhaitable, dans les cas où des fraudes relatives aux ordinateurs ont permis de réaliser des profits considérables, que le malfaiteur puisse être dépouillé de ses profits. Il faudra cependant déterminer si les dispositions actuelles du Code criminel permettent cette mesure et c'est là une autre raison pour laquelle il faut accorder toute la considération voulue à une approche multivalente qui permettrait une réparation et un redressement appropriés selon le cas. Il convient, je crois, de signaler que des moyens très efficaces de dépouiller les malfaiteurs de profits réalisés de manière frauduleuse ont été adoptés aux États-Unis sous forme d'amendements à la Loi américaine sur les droits d'auteur en 1980.

Enfin, pour ce qui est de la question de l'évaluation, j'aimerais simplement signaler que nous partageons certaines des préoccupations que M. Beatty a soulevées dans son exposé sur la question. Je crois que nous avons trouvé une solution quant aux dispositions sur les méfaits et leur incidence sur la juridiction d'un tribunal et M. Piragoff parlera de cette question. Toutefois, en ce qui concerne les sanctions criminelles, ces dernières revêtent habituellement une plus grande importance dans le contexte de la réparation, encore plus importantes même que les remèdes civils, pour ce qui est d'arriver à une mesure de redressement réaliste, et même encore plus que dans le domaine de juridiction.

La seule observation que j'ai à faire sur les exigences en matière de divulgation est ceci: il est ressorti de nos consultations aux États-Unis avec un représentant du F.B.I. que les pressions que cet organisme a exercées pour essayer d'obtenir des exigences en matière de dénonciations se fondaient en grande partie sur cette base. Si l'on part de l'hypothèse qu'il sera possible d'adopter de nouvelles lois et de nouvelles sanctions, comment pourra-t-on évaluer ces nouvelles mesures si le taux de poursuite n'augmente pas? Devrons-nous arriver à la conclusion que la nouvelle loi n'était pas nécessaire? Que les victimes persistent à ne pas signaler ce genre de fraude? Sur quelles bases pourrions-nous nous fonder pour évaluer les changements ou l'absence de changements? C'est donc la raison invoquée pour obtenir la divulgation obligatoire.

Nous avons adopté une autre stratégie importante, et c'est d'essayer de coordonner toutes les initiatives fédérales qui ont eu une incidence sur notre problème. Ces dernières comprennent les nouvelles lois sur l'accès à l'information, les lois de protection de la vie privée et l'existence de diverses catégories d'informations, à savoir, les secrets de fabrication, les secrets

[Text]

the like. An attempt has been made to assess the amount of personal and/or secret and/or confidential information which is in place in the commercial and public institutions, and to assess the protections already in place in relation to that information.

The reason for that is that it may be that this assessment will show us clearly what needs to be accorded proprietary status, what types of information need to be accorded that status, rather than all information, and what information already has protection and does not require any further protection.

• 1555

There is the revision of the Copyright Act, Madam Chairman, which is important—and I do not know, you may wish to have some information on this, but we consider it to be important because there are in existence criminal sanctions in the existing Copyright Act which will be, we expect, the subject of revision.

To ensure all federal government initiatives are reflected in our project and the solutions which we hope to develop, an interdepartmental committee has been established. The members of this committee are from the Department of Justice, the Ministry of the Solicitor General, the Department of Consumer and Corporate Affairs, the Department of Communications, and the Law Reform Commission of Canada.

It is our view that a comprehensive and integrated approach to the problem of computer technology and its impact on the law in societies as a whole is the appropriate approach. This approach should enable us at least to catch up with the technology, or, if we are fortunate, we may be able to keep pace with the changing technology and to reflect the values of an information society, as this society must now be described.

I would like briefly to turn to the developments in the United States. That jurisdiction seemed a logical jurisdiction to explore, because of our common borders, the reciprocal flow of technology, the vast amount of information exchanged, on a daily basis, and clearly a need to develop mutual responses to a common problem. To that end we consulted with and obtained the assistance of two experts: Susan Nijhowne whose name we have provided the committee with as a possible witness . . . She has considerable experience in research and computer abuse and has partaken in the evolution of legislative schemes in California and at the federal level and has in fact provided testimony to a subcommittee of the judiciary committee of the Senate.

We also attended a symposium on computer crime and privacy at the Brookings Institution in November last year. That seminar was attended by legal experts from the federal government, both the executive and legislative branches, members of the information-processing associations, law enforcement agencies, industry, universities, and research institutions. They reported on the existing situation in computer crime and the role of legislative remedies at all levels

[Translation]

officiels et ainsi de suite. Des efforts ont été faits pour essayer d'évaluer la somme de données personnelles, secrètes ou confidentielles qui existent dans les institutions commerciales et publiques et pour essayer d'évaluer les mesures de protection qui existent déjà eu égard à ce genre d'information.

Nous avons décidé de procéder ainsi parce que nous pensons que cette évaluation fera ressortir clairement les types de renseignements qui doivent être considérés comme des biens privés, par opposition à la somme totale des informations, et les catégories d'informations qui sont déjà protégées et qui n'ont pas besoin de protection supplémentaire.

La Loi sur le droit d'auteur est en cours de révision, madame le président, et cela est important car certaines dispositions pénales actuelles seront certainement modifiées.

Un comité interministériel a été créé afin de s'assurer que toutes les initiatives du gouvernement fédéral se reflèteraient dans notre projet et dans les solutions que nous avons l'intention d'élaborer. Ce comité est composé de représentants du ministère de la Justice, du ministère du Solliciteur général, du ministère de la Consommation et des Corporations, du ministère des Communications et de la Commission canadienne de réforme du droit.

A notre avis, la solution consiste à adopter une approche globale et intégrée vis-à-vis du problème que pose la technologie informatique et son impact sur la législation des sociétés dans leur ensemble. En effet, une telle approche tout au moins nous permettre de rattraper notre retard dans ce domaine et, avec un peu de chance, d'évoluer avec le progrès technologique et d'identifier les valeurs de la société de l'information, comme on l'appelle maintenant.

Permettez-moi de parler quelques instants de l'expérience américaine. Cette comparaison semble tout à fait logique, étant donné que nous partageons des frontières, que nous échangeons des technologies et des informations, quotidiennement, et que nous devons donc chercher ensemble des solutions à ce problème qui nous est commun. Dans cette optique, nous avons demandé, et obtenu, l'aide de deux experts: Susan Nijhowne, que nous avons proposée au comité comme témoin. Elle a en effet une expérience considérable dans le domaine de la «truandique» et a participé à l'élaboration de schémas législatifs en Californie et au niveau fédéral; elle a même témoigné devant un sous-comité du Comité sénatorial sur la Justice.

Nous avons également assisté à un symposium sur les délits reliés aux ordinateurs, à «Brookings Institution», en novembre 1982. A ce colloque assistaient des spécialistes juridiques du gouvernement fédéral, à la fois de l'exécutif et du législatif, des membres d'associations sur le traitement de l'information, d'organismes d'exécution de la loi, de l'industrie, des universités et d'établissements de recherche. Des rapports ont été faits sur la situation actuelle dans ce domaine ainsi que sur le rôle des solutions législatives qu'on peut envisager à tous les paliers

[Texte]

of government, and on the improved implementation of existing laws.

In addition, we were able to have discussions with officials of the federal Department of Justice, the FBI, and with the staff of Representative Bill Nelson, who sponsored the Florida legislation and who has now taken over sponsoring what was known originally as the "Ribicoff bill" in the federal jurisdiction. Although the Ribicoff bill did not pass at the federal level, it clearly appears to have been the basis for most of the state legislative initiatives, the notable exception being that of Florida. I have recently received communications that Representative Nelson has reintroduced a revised version of his bill in Congress on January 31, 1983, and he indicates that he hopes for House passage of this bill sometimes later this year.

In addition to Representative Nelson's efforts to have a bill covering the federal jurisdiction, some 18 states have enacted legislation to deal with the problem of computer abuse. Ms Gilhooly will summarize the various approaches used in those states. However, our attempts to obtain information on the impact of the state legislation have not been successful.

• 1600

It appears from our inquiries that very few cases have been prosecuted under the new legislation. One researcher in California has to date indicated that he has identified only 12 cases covering the period 1979 to the present when the earliest state legislation was put in place. A project is now under way at the Stanford Research Institute to assess the impact of state legislation in a formal way and we hope to get information from that study.

Madam Chairman, I think it could be fair to say that our investigations have revealed that most experts in the United States have described the approach taken by the states as merely knee-jerk responses... that is, no conceptual broad analysis was undertaken—and some experts have stated that more could be done in the area of security techniques and mechanisms to reduce the incidence of computer abuse. In summary, it appears that in some of the states a disjointed, multi-legal approach now provides some protection against computer abuse, and I would just like to indicate the various vehicles that exist in some of the states.

The first is the fact that there is the federal Privacy Act, which has criminal sanctions and therefore the information covered by that statute provides criminal sanctions. Then you have the traditional criminal law state larceny and theft laws, which our information suggests are being used, even today, more than the new computer crime legislation. Then you have the state civil law protection through common law trade secrets, and what has now developed in some states is a uniform trade secrets act which criminalizes; that is, it has criminal sanctions against the acquisition, disclosure and destruction of trade secrets, which has a very broad definition. Then there is the computer crime legislation, which varies across the spectrum of these 18 states, and, as I said, there are not very many reported cases in court. Then you have the federal copyright law which operates. So that, basically, is a picture of the types of protection which exist.

[Traduction]

gouvernementaux; il fut également question de l'amélioration des lois actuelles.

De plus, nous avons pu rencontrer des représentants du Département américain de la justice, du FBI, du représentant au Congrès Bill Nelson, lequel a parrainé la loi de l'État de Floride et qui s'occupe maintenant de ce qu'on appelait au début le «Bill Ribicoff» au niveau fédéral. Certes, ce bill Ribicoff n'a pas été adopté, mais il semble avoir servi de fondement à la plupart des mesures législatives prises par les États, la seule exception notable étant l'État de Floride. J'ai récemment appris que M. Nelson a redéposé une version révisée de son projet de loi au Congrès, le 31 janvier dernier, et qu'il espère que cette nouvelle version sera adoptée au cours de l'année.

Outre les efforts de M. Nelson pour faire adopter un projet de loi au niveau fédéral, environ 18 États ont adopté des lois dans le domaine des crimes reliés aux ordinateurs. M^{me} Gilhooly va vous résumer les différentes approches adoptées par ces États. Cependant, nous n'avons pas réussi à obtenir des informations sur l'impact de ces lois.

D'après ce que nous avons appris, très peu de poursuites ont été intentées en vertu de ces nouvelles lois. Un chercheur en Californie a indiqué que, jusqu'à présent, il n'avait relevé que 12 cas entre 1979 et maintenant, c'est-à-dire depuis qu'une loi a été adoptée dans ce domaine par un État. L'institut de recherches Stanford poursuit des recherches sur l'impact des lois adoptées par les États, et nous espérons pouvoir obtenir des renseignements à ce sujet.

Madame le président, d'après les recherches que nous avons effectuées, la plupart des experts américains qualifient l'approche adoptée par les États comme une réaction au coup par coup, c'est-à-dire qu'ils n'ont pas fait une analyse conceptuelle générale; selon plusieurs experts, il devrait être possible d'améliorer les techniques et mécanismes de sécurité afin de réduire le nombre des délits reliés aux ordinateurs. En résumé, il semble que dans certains États, un mécanisme mixte offre maintenant une certaine protection contre les délits reliés aux ordinateurs, et c'est de ces mécanismes que je vais vous parler maintenant.

Permettez-moi tout d'abord de vous signaler qu'au niveau fédéral, la «Privacy Act» contient des sanctions criminelles et, en conséquence, les informations relevant de cette loi peuvent être assujetties à ces dispositions. Vous avez ensuite le droit pénal traditionnel des États qui régleme les délits de vol, et d'après ce que nous avons appris, ils ont toujours davantage recours à ces lois qu'aux nouvelles lois sur les crimes reliés aux ordinateurs. Vous avez ensuite le droit civil des États, qui protège les secrets commerciaux en vertu de la *common law*; plusieurs États ont d'ailleurs adopté une loi uniforme sur les secrets commerciaux, loi qui contient des dispositions pénales, c'est-à-dire que quiconque achète, divulgue et détruit des secrets commerciaux est passible de sanctions. C'est une définition très vague. Il y a ensuite les lois sur les délits reliés aux ordinateurs, et des lois de ce genre ont été adoptées dans 18 États; toutefois, comme je l'ai dit tout à l'heure, peu de

[Text]

We would like to record the co-operation which we have received from the personnel of public and private institutions in the United States and the interest which they have shown and continue to show in the work of the computer abuse project. It certainly has been a very productive exercise.

Finally, Madam Chairman, I would like to indicate the nature of our consultation. The major consultation in Canada took place earlier this month when a national consultation was held under the auspices of the Department of Justice and the Canadian Information Processing Society. We are happy to be able to say that the consultants were generally in agreement with our approach. Some work needs to be done because, as was to be expected with experts such as we had present, they were able to contribute new ideas and to offer constructive criticism on some of our proposals. In addition, some 17 written proposals were received and are now the subject of analysis and review.

I would just like to indicate the people with whom we have consulted so you might be able to determine in your own judgment whether any of these might be of assistance to the committee. Apart from Dr. Parker of the United States, we also consulted Dr. Willis Ware of Rand Corporation, who gave the keynote address at the Brookings Institution and is regarded as one of the premier experts in the United States in this area.

• 1605

We also consulted Dr. John Teron of the University of Western Ontario, the staff of Representative Bill Nelson of Florida, a member of the staff of the Senate Judiciary Committee, Mr. William Bazie of the FBI, Mr. Roger Olson, Assistant United States Attorney General. We also consulted various representatives from industry, banking, the Canadian Information Processing Society and law enforcement institutions who were in attendance at the Brookings Institution seminar. We have also consulted the Canadian Association of Law Teachers, and the RCMP.

At the national consultation, representatives were present from the Canadian Bankers' Association, the Canadian Depository Association, the Canadian Depository for Securities Limited, the Canadian Bar Association, Statistics Canada, the Canadian Industrial Security Association, the Canadian Organization for Advancement of Computers in Health, the Alberta Hospital Association, the Canadian Association of Data Processing Service Organizations, the Canadian Business Equipment Manufacturers Association, the CIPS Security Special Interest Group and, in particular, Mr. Finch, Mr. Rouse and Miss Woodhead. In our view, Mr. Rouse was extremely helpful and continues to be extremely helpful to us, as we evaluate some of the suggestions from that consultation.

[Translation]

poursuites ont été intentées en vertu de ces lois. Il ne faut pas oublier non plus la loi fédérale sur le droit d'auteur, qui est toujours en vigueur. Voilà donc un bref tableau des mécanismes législatifs en place.

Permettez-moi ici remercier publiquement le personnel des établissements publics et privés des États-Unis pour la collaboration qu'ils nous ont offerte et pour l'intérêt qu'ils ont su manifester, et qu'ils continuent de manifester, à l'égard du projet sur les délits reliés aux ordinateurs. C'est un exercice qui a été extrêmement fructueux.

Pour terminer, madame le président, je voudrais vous dire quelques mots sur les consultations que nous avons effectuées. La principale que nous ayons faite au Canada a eu lieu au début du mois, lorsqu'une consultation nationale a été organisée sous les auspices du ministère de la Justice et de la *Canadian Information Processing Society*. Nous sommes heureux de pouvoir vous dire que notre approche a fait l'objet d'un consensus parmi les experts-conseils. Certes, il y a encore du travail à faire car les experts qui étaient présents à cette conférence ont su nous donner des idées novatrices, tout en nous faisant des critiques constructives sur certaines de nos propositions. De plus, nous avons reçu 17 propositions écrites que nous sommes en train d'analyser.

Permettez-moi maintenant de vous parler de ceux que nous avons consultés, afin que vous puissiez déterminer si ces personnes pourraient éventuellement être utiles à votre Comité. Outre M. Parker des États-Unis, nous avons consulté M. Willis Ware de la Rand Corporation, qui a fait la principale communication lors de la conférence qui a eu lieu à Brookings Institution, et qui est considéré comme l'un des grands experts américains dans ce domaine.

Nous avons également consulté M. John Teron de l'Université de l'Ouest de l'Ontario, le personnel du représentant de la Floride, Bill Nelson, un membre du personnel du comité judiciaire du Sénat, M. William Bazie du FBI, M. Roger Olson, procureur général adjoint des États-Unis. De plus, nous avons consulté des représentants de différents secteurs de l'industrie, des banques, de la *Canadian Information Processing Society* ainsi que des institutions d'application de la loi qui assistaient au séminaire de l'Institution Brookings. Nous avons également consulté l'Association canadienne des professeurs de droit ainsi que la GRC.

Quant à la consultation nationale, y assistaient des représentants de l'Association des banquiers canadiens, de l'Association canadienne des dépôts, de la Société *Canadian Depository for Securities Limited*, de l'Association du Barreau canadien, de Statistique Canada, de l'Association canadienne pour la sécurité industrielle, de l'Organisation canadienne pour promouvoir les ordinateurs dans le domaine de la santé, de l'Association des hôpitaux de l'Alberta, de l'Association canadienne du traitement des données, de l'Association canadienne des manufacturiers de matériel de bureau, du groupe spécial chargé de la sécurité du CIPS, et, en particulier MM. Finch et Rouse ainsi que M^{me} Woodhead. Nous avons trouvé l'intervention de M. Rouse particulièrement utile et va

[Texte]

There was also a representative from the CIPS Special Security Interest Group from Montreal, and from Calgary, there was a representative from the Commercial Security Association, the Canadian Institute of Chartered Accountants, the Association of Record Managers and Administrators, the Canadian Industrial Communications Assembly, the Canadian College of Health Record Administrators, as well as from the Universities of Toronto, Calgary, Guelph, British Columbia, Manitoba, Saskatchewan. The Deputy Chief of Police, Mr. Thomas Flanagan, represented the Canadian Association of Chiefs of Police. The Ontario Provincial Police were represented. The RCMP were represented. There were least two computer experts from the private sector, Gulf Canada, the Canadian Imperial Bank of Commerce, the Bank of Montreal.

That group of experts with so many different interests and different aspects to the problem met with us. We held a successful consultation, and it is in that context that we sincerely hope that the proposals which we develop will reflect the contribution of so many people who have been of assistance to us. We certainly take pleasure in providing you with that input as well so that, together, we may be able to provide the best possible solution to what is clearly and admittedly a complex problem. Thank you, Madam Chairman..

Le président: Merci, monsieur Hill. Est-ce que mes collègues ont des questions?

Mr. Beatty: Is there more to the presentation, or was that it?

Mr. Hill: That is our presentation.

Mr. Beatty: Perhaps I could get some guidance from you, Madam Chairman. Are we expecting to deal with another group of witnesses today?

The Chairman: For me, I am willing to stay until 5.00 p.m..

Mr. Beatty: Unfortunately, I am going to have to go at about 4.30 p.m. so I guess what we should do is concentrate on this.

The Chairman: Maybe I will let you ask the questions until 4.30 p.m., and if I have a few questions, I will have an exchange with the witnesses after. But it is all recorded so you can have the written document afterwards.

Mr. Robinson (Etobicoke—Lakeshore): But the other witnesses today will have to come back another day, will they not? There just is not sufficient time for us to listen to them or to question them.

The Chairman: I do agree. But the problem is, I presume, that in order not to have repetition and, since they are working together, if we want to have them back, we will decide at a later date. But if we want to ask questions today of the RCMP... I do not know; do you have a presentation?

[Traduction]

continuer à l'être quand on va évaluer les suggestions qui ont été faites lors de cette consultation.

Il y avait également un représentant du groupe spécial de sécurité du CIPS, il venait de Montréal et, étaient venus de Calgary, un représentant de l'Association de la sécurité commerciale, de l'Institut canadien des comptables agréés, de l'Association des gérants et administrateurs de dossiers, du Groupe canadien des communications industrielles, du Collège canadien des administrateurs de dossiers de la santé ainsi que des Universités de Toronto, de Calgary, de Guelph, de Colombie-Britannique, du Manitoba et de la Saskatchewan. Le sous-chef de police, M. Thomas Flanagan, représentait l'Association canadienne des chefs de police. La Police provinciale de l'Ontario était également représentée, ainsi que la GRC. Assistaient également à la réunion au moins deux experts en informatique du secteur privé, des représentants de Gulf Canada, de la Banque canadienne impériale de commerce et de la Banque de Montréal.

Ce groupe d'experts venant de secteurs si différents et ayant des intérêts si divers sont venus discuter avec nous du problème. La consultation a été fort utile et nous espérons que les propositions que nous formulerons à la suite de cet exercice seront le reflet fidèle des opinions de toutes ces personnes qui nous ont aidés. En tout cas, c'est un plaisir de vous soumettre les résultats de cette participation pour que nous puissions travailler ensemble à la recherche de la meilleure solution possible pour ce problème évidemment très complexe. Merci, madame le président.

The Chairman: Thank you, Mr. Hill. Do my colleagues have any questions to ask?

M. Beatty: Avez-vous quelque chose à ajouter ou bien votre exposé est-il terminé?

M. Hill: C'est terminé.

M. Beatty: Madame le président, pouvez-vous nous dire si nous attendons un autre groupe de témoins?

Le président: Personnellement, je suis prête à rester là jusqu'à 17 heures.

M. Beatty: Malheureusement, je dois m'absenter vers 16h 30 si bien qu'il vaudrait mieux nous en tenir à cette question.

Le président: Dans ce cas, peut-être pourriez-vous poser vos questions jusqu'à 16h30 puis, si j'en ai moi-même, je les poserai quand vous serez parti. De toute façon, elles seront enregistrées et vous pourrez les lire par la suite.

M. Robinson (Etobicoke—Lakeshore): Mais les autres témoins devront revenir un autre jour, n'est-ce pas? Nous n'avons tout simplement pas le temps de les entendre et de poser des questions aujourd'hui.

Le président: Je suis bien d'accord. Le problème, c'est que tous ces gens-là travaillent en collaboration et nous risquons d'entendre les mêmes choses plusieurs fois. Nous pourrions toujours décider plus tard si nous voulons les réinviter. Cela dit, si nous avons des questions à poser à la GRC aujourd'hui... Je ne sais pas. Vous avez un exposé?

[Text]

• 1610

Superintendent George Allen (Commercial Crimes Branch, Royal Canadian Mounted Police): Yes, I do Madam Chairman, it takes about 20 minutes, roughly.

Mr. Beatty: If it is just 20 minutes, I wonder whether, Madam Chairman, it might be useful to have that presentation on the record and hold questions over to another day. It would give us a chance to study the record.

The Chairman: It is up to you.

Mr. Beatty: That would be my suggestion.

Mr. Robinson (Etobicoke—Lakeshore): I think so; then it might be that they would want to come back and we could ask the questions. We are just not going to have enough time to ask questions today and to hear them as well.

Mr. Beatty: There is also a good deal of material that was presented in a written form that we would have a chance to take a look at.

Mr. Hill: Yes, and our presentation has not been completed, because we have other witnesses who put everything together.

The Chairman: No problem with me.

Mr. Beatty: If it is acceptable, perhaps we could hear as well, then, from the RCMP today.

The Chairman: Okay, fine. You can stay at the table, Mr. Hill.

Mr. Hill: I am much obliged.

Le président: Je souhaite maintenant la bienvenue au surintendant George Allen de la Section des délits commerciaux de la Gendarmerie royale du Canada.

Monsieur Allen, vous avez la parole.

Sdt George Allen: Merci, madame le président.

Madam Chairman, and members of the subcommittee, thank you for the opportunity to appear before you to present the Royal Canadian Mounted Police position on this important issue. I trust that our comments and recommendations will assist the committee in its deliberations.

As you are aware, the electronic age has arrived. *Time* magazine has recently named the computer as their "Man of the Year" and it is, indeed, timely that this important topic receives a thorough examination.

Police statistics do not support the suggestion that there is a serious problem with respect to the use of computers in criminal activities. Nevertheless, the RCMP has been devoting an increasing number of hours to investigations and, along with the proliferation of personal and corporate computers, supports the view that crimes involving computers and electronic data need to be seriously addressed through improved security and legislative action to protect those who may be victimized. For the most part, poor application of

[Translation]

Le superintendant George Allen (Section des délits commerciaux, police montée canadienne): Oui, madame le président, et j'en aurai pour une vingtaine de minutes.

M. Beatty: Si cela ne dure que vingt minutes, madame le président, nous ferions peut-être mieux d'écouter cet exposé tout de suite et de réserver nos questions pour un autre jour. Cela nous permettrait de nous familiariser avec ce qui aura été dit.

Le président: C'est à vous d'en décider.

M. Beatty: C'est ce que je pense.

M. Robinson (Etobicoke—Lakeshore): C'est une bonne idée. Les témoins accepteront peut-être de revenir pour répondre aux questions. Aujourd'hui, nous n'aurons tout simplement pas le temps de poser des questions et d'entendre l'exposé.

M. Beatty: Il y a également beaucoup de documents écrits qui ont été soumis; cela nous donnerait le temps de les lire.

M. Hill: Effectivement, et notre exposé n'est pas terminé parce que nous avons d'autres témoins qui ont rassemblé toutes les données.

Le président: Je n'y vois pas d'inconvénient.

M. Beatty: Dans ce cas, nous pourrions également écouter les représentants de la GRC aujourd'hui.

Le président: Parfait. Monsieur Hill, vous pouvez restez là.

M. Hill: Je vous remercie.

The Chairman: I now welcome Superintendent George Allen, from the Commercial Crimes Branch of the Royal Canadian Mounted Police.

Mr. Allen, you have the floor.

Supt George Allen: Thank you, Madam Chairman.

Madame le président et membres du Sous-comité, nous vous remercions de cette occasion de comparaître et de vous expliquer la position de la Gendarmerie royale du Canada face à cet important problème. J'espère que nos observations et nos recommandations pourront vous être utiles dans vos délibérations.

Comme vous le savez, l'ère de l'électronique est arrivée. Le magazine *Time* vient de choisir l'ordinateur comme «Homme de l'année» et il est donc particulièrement opportun de réfléchir à cette question.

Les statistiques de police nient que l'utilisation illégale de l'ordinateur constitue un problème grave. Néanmoins, la GRC consacre de plus en plus d'heures de travail à des enquêtes dans ce domaine et la prolifération des ordinateurs domestiques et industriels prouve qu'il est temps de s'intéresser à cette importante question et d'étudier des mesures de sécurité, des mesures législatives pour protéger les futures victimes. Jusqu'à présent, dans la plupart des cas, des mesures de sécurité mal appliquées ont été à l'origine des plaintes, mais ce n'était pas la

[Texte]

security measures has been the cause of complaint and has resulted in otherwise appropriate security being compromised. While we support the need for legislation, it is not the only answer to the problem, because the first line of defence rests with the victim.

The types of criminal offences involving a computer are generally seen as: one, where the computer is the object of the crime;

Two, where we have the computer as the victim of a crime;

Third, where the computer itself is used as a tool to commit the crime.

Where the computer is the object of the crime: Acts directed to computer hardware are treated quite adequately under current legislation. The act is a human, observable occurrence; it results in harm or loss of a standard type. However, it should be clearly understood that this is only with respect to the physical equipment and does not include the data or programs stored within a computer system.

The computer as a victim of the crime: This area deals primarily with the unauthorized use of a computer system, be it to run personal programs or to scan the data banks resident within the system.

Unauthorized use from within the organization: Within the EDP environment, different levels of access are authorized according to a person's position within the company. Corporations are rightfully worried about what to do when employees deliberately exceed their prescribed authorities and use the system for personal reasons or to access and copy information to which they are not entitled. While this is a major area of concern, the prime responsibility must remain with industry to take all the necessary measures to protect itself, because this type of activity does not constitute a criminal offence at this time. Law enforcement agencies would continue to provide assistance in a crime prevention role.

The unauthorized use from outside the organization: With the introduction of communications into the computer field, the whole concept of information protection, as we have traditionally known it, has changed. One of the most important assets in the modern corporation is information, and until recently the standard procedures were to place the vital information in a locked safe and the building itself secured through conventional means. Thus, the principles of protection arising from the medieval fortress have remained the pillar of today's security.

With the advent of modern technology, it is now possible to enter computer systems and obtain all the information from the system's data bank without once having to approach or breach the conventional security barriers. Here again, the victims have the primary responsibility to ensure the use of electronic codes and passwords controlling access to their

[Traduction]

qualité de cette sécurité qui était en cause. Nous reconnaissons que de nouvelles lois doivent être adoptées, mais ce n'est pas la seule solution du problème car le principal moyen de défense est entre les mains de la victime.

Dans le domaine des ordinateurs, il y a plusieurs types de délits: premièrement, lorsque l'ordinateur est l'objet du délit;

deuxièmement, lorsque l'ordinateur est la victime du délit;

troisièmement, lorsque l'ordinateur proprement dit est utilisé comme outil pour perpétrer le délit.

Lorsque l'ordinateur est l'objet du délit, la législation actuelle relative au matériel informatique est tout à fait suffisante. Le geste est posé par un être humain et est observable; son résultat est un dommage ou une perte d'un type reconnaissable. Toutefois, il faut bien comprendre que cela s'applique uniquement au matériel et ne comprend pas les données ou programmes entreposés dans un système d'ordinateur.

L'ordinateur en tant que victime d'un délit: dans ce cas, il s'agit surtout de l'utilisation non autorisée d'un système d'ordinateur, que ce soit pour utiliser des programmes personnels ou pour la consultation de banques de données confiées au système.

L'utilisation non autorisée au sein de l'organisation: dans une entreprise privée informatisée, chaque employé reçoit un degré d'accès à l'ordinateur qui dépend de son poste dans la hiérarchie de la compagnie. Les sociétés s'inquiètent de mesures à prendre lorsque des employés dépassent délibérément leur limite d'accès pour utiliser le système à des fins personnelles ou encore pour y obtenir des informations auxquelles ils n'ont pas droit. C'est sans doute une préoccupation importante, mais c'est tout de même au secteur privé d'en assumer la responsabilité et de prendre les mesures nécessaires pour se protéger; en effet, jusqu'à présent, ce type d'activité n'est pas considéré comme un délit criminel. Les organismes d'application de la loi sont toutefois disposés à poursuivre leurs efforts dans le domaine de la prévention.

Accès non-autorisé de l'extérieur de l'organisation. Avec l'arrivée de la téléinformatique tous les principes traditionnels de protection ont été modifiés. L'information est devenue l'un des outils les plus importants de l'entreprise moderne et, jusqu'à tout récemment, la procédure la plus généralement acceptée était d'enfermer les informations dans un coffre-fort et d'assurer la sécurité de l'immeuble par des moyens conventionnels. Ainsi, les principes de protection qui avaient leur origine dans la forteresse médiévale sont encore les piliers de la sécurité moderne.

Avec l'arrivée d'une nouvelle technologie, il est maintenant possible de pénétrer dans un système d'ordinateur pour en recueillir les informations sans devoir affronter une seule fois les barrières conventionnelles de sécurité. Là encore, c'est avant tout aux victimes de se protéger par la mise en place de codes électroniques et de mots de passes, de contrôler l'accès à

[Text]

systems and to implement a good sound security policy that is updated regularly.

There are several areas of major concern with respect to the unauthorized use from outside the organization.

First, obtaining computer services: A case in point involved the students of a school in New York City wanting more computer time than was allotted to them by the school. Knowing the access protocols for the Canadian computer communications network, they accessed this network in search for a computer that was using an operating system with which they were familiar. Having located one, they effectively became the controller of the computer and proceeded to use it for their own purposes. This modus operandi is evident in several other cases reported to the RCMP. We perceive these cases being reported as a result of the inability on the part of private institutions to deal with the matter internally.

The second area is commonly referred to as "system hacking". There exists within the United States a loosely affiliated group that refers to itself as "hackers". Their ultimate goal is to try to penetrate as many computer systems as possible, and once they have succeeded they leave information as to how it was accomplished at the various electronic bulletin boards that exist throughout Canada and the United States. These bulletin boards are merely data banks which are accessible by anyone who has a dial-operated computer terminal and are legitimately used by many corporations for purposes of electronic mail.

The results of the hackers' practices are somewhat difficult to ascertain, but in one instance at a Canadian service bureau the system was being so greatly hampered by the number of hackers who were regularly accessing it from all over the United States that the company was unable to service its paying customers. The victim company in this particular case has declined to involve the police in its problem due to the danger of adverse publicity impairing its business. It is our opinion, however, that one of the motivating factors in the refusal to invoke the criminal process is the belief that the laws are inadequate to effectively deal with this type of criminality.

The third area is industrial espionage. Since many corporations maintain large amounts of valuable and/or sensitive data in their computerized data banks, these systems become a prime target for espionage. While no reported incidents are on file with the RCMP, there have been convictions in the United States under their industrial espionage laws, and we must therefore assume that there is a great potential for similar acts in Canada.

The fourth area is sabotage of computer operations or information. Sabotage in this context refers to two separate and distinct activities that can be done which would directly affect the computer operations.

[Translation]

leurs systèmes et d'adopter une politique fiable de sécurité et de la réviser fréquemment.

Ce ne sont pas les seuls problèmes posés par l'accès sans autorisation de l'extérieur de l'organisation.

Premièrement, accéder aux services d'ordinateur. Je vous cite un exemple, des étudiants d'une école de la ville de New York réclamaient plus de temps d'ordinateur que l'école n'était prête à leur accorder. Connaissant les protocoles d'accès au réseau de communication informatique canadien, ils pénétrèrent dans le réseau pour y trouver un ordinateur dont le système leur soit familier. Ayant trouvé cet ordinateur, ils en prirent le contrôle et commencèrent à s'en servir à des fins personnelles. Ce n'est pas un cas isolé, la GRC en a plusieurs autres exemples. Si nous entendons parler de ce genre de chose, c'est sûrement parce que les institutions privées ne trouvent pas de solution interne aux problèmes.

Le second phénomène est souvent désigné sous le terme de «piochage du système». Aux États-Unis, il y a un groupe vaguement affilié qui se désigne lui-même sous le thème «piocheur». Leur but est de s'infiltrer dans le plus grand nombre de systèmes d'ordinateurs possibles et, lorsqu'ils y ont réussi, d'afficher des notices sur les différents tableaux d'affichage électronique du Canada et des États-Unis pour expliquer comment ils s'y sont pris. Ces tableaux d'affichage sont en réalité des banques de données accessibles à quiconque peut utiliser un terminal d'ordinateur avec cadran et sont utilisés par beaucoup de sociétés pour leur courrier électronique.

Les résultats des activités des piocheurs sont un peu difficiles à établir, mais je sais qu'à un moment donné, un bureau de service canadien fut tellement désorganisé par le nombre des piocheurs qui s'infiltraient dans le système de partout aux États-Unis, qu'il lui était devenu impossible de desservir ses clients payants. Dans ce cas particulier, la compagnie victime refusa de faire appel à la police craignant les résultats d'une publicité négative. Toutefois, nous estimons que très souvent les gens qui refusent de se prévaloir du système de justice criminelle agissent ainsi parce qu'ils pensent que les lois sont insuffisantes pour les protéger efficacement contre ce type de délit.

Le troisième problème est celui de l'espionnage industriel. Beaucoup de sociétés gardent des masses de données très précieuses dans leurs banques de données informatisées; ces systèmes deviennent des cibles de choix pour l'espionnage. La GRC n'en a pas d'exemple dans ses dossiers, mais aux États-Unis plusieurs personnes ont été reconnues coupables d'infractions aux lois sur l'espionnage industriel et tout porte à croire que le même potentiel existe au Canada.

Le quatrième problème a trait au sabotage des opérations ou de l'information des ordinateurs. Dans ce contexte, quand on parle de sabotage, il s'agit de deux activités bien distinctes qui, toutes deux, peuvent porter atteinte aux opérations de l'ordinateur.

[Texte]

• 1620

One of these is to access a computer system and alter or erase programs or data banks, so that when jobs are run they either produce incorrect results or they fail to work at all. The other procedure is to enter specific routines or instructions during peak usage periods that cause the computer to cease function, or as it is referred to in the vernacular of the EDP environment, to cause a "system crash." A prime example of this situation is where a person systematically caused a university computer system to crash, thereby rendering the facility unavailable to the mass of students who were supposed to use it to prepare assignments.

Because of the inherent problems involved in these system crashes, computer centres traditionally make regular copies of their data which can be used to reconstruct the data base in the event it is lost. Notwithstanding the backup, the reconstruction of the computer data base can be an expensive proposition, while the location of program changes can be even more costly to a user since it involves the total analysis of the programs to find out what changes were made.

A system crash does not usually render the computer permanently out of commission, but the system remains unavailable to the users until computer technicians re-initialize the system in what is referred to as "re-booting the system" or "doing a dead start." This procedure can take considerable time to effect.

In all the situations where the computer is victimized from outside the organization, there appear three major problems from an investigational standpoint. These are the interception of the computer transmission, identification of the perpetrator and the location of operations, and thirdly, proof that the act committed is a crime.

Modern technology has enabled common carriers to develop a computer communication system commonly referred to as "packet switching," which is a method whereby all transmissions are sent through common lines at high speeds, with addresses on each packet as to the originator and recipient. In essence, the communication network is somewhat analogous to a postal system, where each computer and terminal is assigned a box number or address and the various packets of information are the letters flowing between the various addresses.

The RCMP has encountered a problem with respect to an authorization under Part IV.1 of the Criminal Code with respect to computer communications, because of the inherent properties of the packet-switching network and because, in the opinion of a particular judge, an authorization to intercept would in essence be allowing the police to open all mail being transmitted from the terminal, be it legitimate or not.

This will remain a problem, since many computer terminals are located in general access environments and serve many people within the organization. It therefore becomes impossible to identify the perpetrator without monitoring all

[Traduction]

Une des techniques est de pénétrer un système d'ordinateur et de modifier ou d'effacer des programmes ou des banques de données; lorsque celles-ci sont utilisées par la suite, soit elles donnent des résultats inexacts, soit elles ne fonctionnent pas du tout. L'autre méthode est de pénétrer dans des programmes spécifiques ou des séquences d'instruction pendant les périodes de pointe d'utilisation et l'ordinateur cesse de fonctionner, ce qu'on appelle dans le jargon de l'informatique un «crash» du système. Le meilleur exemple est celui de l'individu qui provoquait un «crash» systématique de l'ordinateur d'une université, empêchant ainsi tous les étudiants qui en avaient besoin pour leurs travaux de s'en servir.

A cause des problèmes inhérents à ces «crash» du système, les centres d'ordinateurs font de façon systématique des copies de leur données, ce qui permet de reconstituer la base de données en cas de perte. En dépit de cette précaution, la reproduction des données d'ordinateur est un processus souvent très coûteux; cela dit, il peut être encore plus onéreux de détecter les changements apportés aux programmes puisque, pour y parvenir, il faut analyser l'ensemble des programmes.

En règle générale, un crash n'empêche pas un ordinateur de fonctionner définitivement, mais tant que les techniciens n'ont pas remis la machine en marche, les usagers ne peuvent plus s'en servir. Or, c'est une démarche qui peut prendre pas mal de temps.

Lorsqu'un ordinateur est victime d'actions parties de l'extérieur de l'organisation, du point de vue de l'enquêteur, trois problèmes principaux se posent: Interception d'une transmission d'ordinateur, identification du coupable et de l'endroit où il se trouve et, troisièmement, preuve que l'action en question est véritablement un délit.

La technologie moderne a permis aux transporteurs modernes de mettre au point un système de communication par ordinateur, que l'on désigne généralement sous le terme de «regroupage». C'est une méthode qui permet d'envoyer toutes les transmissions sur des lignes communes à des vitesses très élevées, chacune d'entre elles portant les adresses de l'expéditeur et du destinataire. Au fond, le réseau de communication ressemble un peu au système postal: chaque ordinateur et terminal est désigné par un numéro ou adresse, et les différents envois d'information sont les lettres qui circulent entre les différentes adresses.

L'autorisation prévue par la Partie IV .1 du code criminel et portant sur les communications par ordinateur a posé un problème à la GRC à cause des caractéristiques inhérentes du réseau de regroupage des expéditions et parce qu'un juge a décidé que l'autorisation d'intercepter était la même chose que si l'on permettait à la police d'ouvrir tout le courrier expédié d'un terminal, légitimement ou pas.

C'est un problème qui est loin d'être résolu, car beaucoup de terminaux d'ordinateur sont situés dans des endroits très accessibles et desservent un grand nombre de personnes appartenant à une organisation. Il devient donc impossible d'identifier un coupable sans surveiller toutes les informations

[Text]

information being transmitted through the system, including that of legitimate users.

Thirdly, the computer as a tool to commit crimes. The RCMP sees this as one of the major areas where the computer will become involved in the crime field. Here again, the implication can be addressed in several areas.

First, the owner modifies for a criminal purpose. A situation where the computer is used as a repository of information or as a data manipulator to either monitor or maintain information and accounting records on criminal activities or to actually perpetrate criminal acts. Prime examples are where bookies maintain their betting records on computer, or where programs used to produce invoices are made to charge more, on the premise that if someone complains it is blamed on computer error.

Secondly, the unauthorized modification for a criminal purpose. The computer is accessed by someone whose actions are designed to benefit himself at the expense of the corporation. Examples are where employees modify money-calculating programs and credit certain portions of the product to their or someone else's account. The prime example of this is in what is generally referred to as the rounding scheme, where interest-calculating programs are modified to deposit the fractions of cents involved in the process to a specific account, which is then subsequently converted by the perpetrator.

• 1625

The RCMP has no record of such types of crime being committed in Canada. However, the scenario has been reported in numerous documented cases in the United States and unofficial reports tend to support the premise that they are occurring in Canada. These unofficial reports are originating at various conferences on computer crimes, where participants relate either their corporate or personal experiences, and in discussion with industry people. While the actual modus operandi will be different in each instance, the ultimate goal is to cause the computer to effect certain changes to money-dispersment routines, billing procedures and internal records.

In all these cases where the computer is used as a tool to commit a crime, the existing laws are adequate to handle the actual crimes, since in these situations the computer is merely ancillary to the crime itself. It is in this area, however, that there are serious evidentiary problems from a law-enforcement perspective.

Current legislative issues: The RCMP perceive the current Canadian legislation as deficient, lacking in direction to both the courts and the police, in three distinct categories which pertain to computers: First, the introduction of computer-generated documents into a court of law; the identification of a computer-related incident as a criminal offence, and, thirdly, the powers of investigation, more specifically search, seizure and intercept of information in computer systems.

[Translation]

qui passent dans le système, y compris celles des usagers légitimes.

Troisièmement, l'ordinateur en tant qu'outil de crime. La GRC estime que c'est l'un des principaux domaines où l'univers de l'ordinateur et celui du crime sont appelés à coïncider. Là encore, les implications sont visibles dans plusieurs domaines.

Premièrement, le propriétaire qui effectue des modifications à des fins criminelles. C'est le cas d'un ordinateur utilisé pour l'entreposage d'informations ou pour manipuler des données, soit pour contrôler des informations ou des dossiers de comptabilité portant sur des activités criminelles ou même encore pour commettre de véritables actes criminels. Prenez l'excellent exemple des bookmakers qui mettent sur ordinateur leurs dossiers de paris et l'exemple des programmes qui sont utilisés pour gonfler des factures, étant bien entendu que, si quelqu'un se plaint, on pourra toujours blâmer l'ordinateur.

Deuxièmement, modification non autorisée à des fins criminelles. Un individu gagne accès à l'ordinateur pour des fins personnelles et aux dépens de la société. Par exemple, les employés qui modifient les programmes financiers pour en créditer une partie à leur compte ou au compte de quelqu'un d'autre. Le meilleur exemple de cela, c'est lorsqu'on modifie les programmes de calcul des intérêts de façon que les fractions de cents soient automatiquement versées à un compte donné que liquide ensuite l'auteur du crime.

La GRC n'est au courant d'aucun crime de ce genre au Canada. Toutefois, la formule est connue aux États-Unis où l'on a pu monter plusieurs dossiers de ce genre et, officieusement, il semble que la même chose se produirait au Canada. Ces rumeurs proviennent des diverses conférences organisées sur les crimes informatiques, où les participants racontent leur expérience personnelle ou l'expérience de leur société, ou alors ils en discutent avec des gens du milieu. La façon de procéder diffère normalement d'un cas à l'autre, mais le but ultime est de commander à l'ordinateur de modifier la façon dont il répartit l'argent, dont il fait les factures et la façon dont il tient les dossiers internes.

Dans tous ces cas-là où l'ordinateur sert de moyen pour commettre un crime, les lois actuelles permettent de traiter le crime même puisque l'ordinateur est alors tout simplement subordonné au crime. Cela pose toutefois de graves problèmes de preuve pour ceux qui ont à faire respecter la loi.

Problèmes posés par la législation actuelle: Pour la GRC, les lois canadiennes actuelles comportent des lacunes, car elles ne peuvent guider ni les tribunaux ni les policiers dans trois domaines distincts qui se rapportent aux ordinateurs. Le premier domaine, c'est le dépôt en cour de justice de documents informatisés; le deuxième, c'est la classification d'un incident lié aux ordinateurs parmi les infractions criminelles; et le troisième, les pouvoirs d'enquête, plus particulièrement la perquisition, la saisie et l'interception de renseignements, dans les systèmes informatiques.

[Texte]

Computer-generated documentary evidence: The Canada Evidence Act provides for the admissibility, under certain circumstances, of copies of records and records as defined in Section 30.(12).

Whether or not a computer-produced document is a record or a copy by this definition is perhaps arguable. With the explosion of electronically stored data in use in industry, this becomes an extremely important question that should not be left open to interpretation.

In summary, computer-generated documentary evidence requires examination and legislative amendment to clarify its admissibility.

Second, the identification of a computer-related incident as a criminal offence: Computer-related incidents may or may not be identifiable as a criminal offence depending on whether hardware or software is involved. There is no doubt that the damage to, or theft of, computer hardware is dealt with through existing legislation. The issue of identifying the incident as an offence arises when dealing with unauthorized use, alteration, destruction, removal or copying of computer software. In addition, software, information/data and programs have been held to not fall within the definition of property for the purposes of either theft or damage offences; consequently, current legislation does not contemplate an offence.

Third, investigative powers in computer-related crimes: With the advent of computer systems, investigating officers are being faced with increasing problems regarding the availability of evidence stored in electronic form. In large automated firms, many written documents that were traditionally used to record corporate transactions are now disappearing as more and more the computer data banks are becoming the sole repository of the information. Both the private and time-sharing systems present major law enforcement problems.

Search and seizure: Traditional search and seizure methods and procedures are not adequate to deal with modern technological advances in the computer field, particularly in cases where information may be stored in more than one location in a computer system and which, in itself, can be located in several jurisdictions or countries. At the present time there are at least 10 corporations in Canada offering service bureau facilities to Canadians where the data banks and computer are located in the United States. We not have any statistics on the number of Canadian subsidiaries of foreign firms using their parent company computer facilities, but it is safe to say that there are many.

The RCMP is concerned about the availability of the computer-stored information that is pertinent to Canadian transactions and possibly crimes committed in Canada. The RCMP is also concerned about the ability to compel Canadian subsidiaries of foreign firms to produce the information resident in computers located outside of Canada.

[Traduction]

D'abord les documents informatisés comme preuve. La Loi sur la preuve au Canada permet d'admettre comme preuve, dans certaines circonstances, des copies de pièces et des pièces, dont la définition se trouve à l'article 30.(12).

On pourrait prétendre qu'un document informatisé est une pièce ou une copie d'une pièce en vertu de cette définition. Depuis l'explosion des données emmagasinées électroniquement dans l'industrie, la question devient extrêmement importante et ne devrait laisser aucune place à l'interprétation.

En résumé, il faut étudier l'admissibilité des documents informatisés à titre de preuve et apporter les amendements législatifs requis pour clarifier la situation.

Ensuite, la classification d'un incident lié à l'ordinateur parmi les infractions criminelles. De tels incidents peuvent être classés ou non comme une infraction criminelle suivant qu'on s'est servi du logiciel ou du matériel. Evidemment, la loi actuelle traite des dommages au matériel et de son vol. Classer un incident comme une infraction criminelle devient difficile quand il s'agit d'usage sans autorisation, de modification, de destruction, de retrait ou de copie de logiciel. De plus, on a déjà jugé que les logiciels, les données et les programmes ne peuvent être compris dans la définition qui est donnée des biens et de la propriété aux fins des infractions criminelles que constituent le vol ou les dommages. Par conséquent, la loi actuelle n'en fait pas une infraction criminelle.

Enfin, les pouvoirs d'enquête sur les crimes informatiques. Depuis l'avènement des systèmes informatiques, les enquêteurs font face à de plus en plus de problèmes à cause de la disponibilité des preuves emmagasinées électroniquement. Dans les grandes entreprises automatisées, la plupart des documents écrits qui servaient traditionnellement de preuve des transactions commerciales disparaissent de plus en plus pour faire place aux banques de données informatisées, qui sont maintenant les seuls dépôts de renseignements. Les systèmes privés, comme les systèmes à temps partagé, posent de graves problèmes à ceux chargés de l'application de la loi.

Les perquisitions et les saisies. Les méthodes et procédures traditionnelles pour la perquisition et la saisie sont incapables de faire face aux progrès technologiques dans le domaine informatique, surtout dans les cas où l'information peut être emmagasinée à plusieurs endroits d'un système informatique, qui lui-même peut se trouver dans des juridictions, voire des pays différents. En ce moment-même, au moins dix sociétés au Canada offrent des services informatiques à des Canadiens, alors que les banques de données et les ordinateurs se trouvent aux États-Unis. Nous n'avons aucune statistique sur le nombre de filiales canadiennes d'entreprises étrangères qui se servent des ordinateurs de leur société mère, mais on peut affirmer, sans risquer de se tromper, qu'il y en a beaucoup.

La GRC s'inquiète donc de la disponibilité des renseignements emmagasinés dans ces ordinateurs, concernant des transactions faites au Canada et des crimes commis ici. La GRC s'inquiète aussi de sa capacité à obliger les filiales canadiennes d'entreprises étrangères de fournir l'information qui se trouve dans ces ordinateurs à l'étranger.

[Text]

Time-sharing also creates its own problems where there is a mix of electronic information, unlike hard-copy material which can be physically segregated where it becomes difficult to avoid accessing other privileged data not covered in the authorization since the only way of ascertaining that all relevant information has been obtained is by examining the entire system. In addition, normal record-keeping and production requirements of federal and provincial legislation need modernizing, such as Section 355 of the Criminal Code.

Lawful Intercept. It is not clear whether or not a transmission between a computer and its terminals, between a terminal and another terminal, or between computer systems, is a private communication within the meaning of current legislation. Consequently, this presents serious problems in gathering evidence and must be addressed to allow effective enforcement measures in computer-related investigations.

The current criminal law in Canada has adequate provisions to identify offences with computer-related crimes where tangible assets are concerned. There are, however, some problems related to the collection and presentation of evidence in relation to those and other offences. The present criminal law is inadequate in dealing with the occurrences involving intangible items, such as information or data in a computerized environment, due to the fact that information is not considered to be property or anything within the interpretations utilized in criminal law.

Simply affording properties status to data or information may not prove suitable for prosecutions under the theft or fraud sections when forced with legal interpretations of taking, copying, translating, or converting something that remains available to the original owner. It would also raise the problem of valuation as an issue at trial. Valuation of data or programs for the purpose of determining the appropriate penalty section under which charges are preferred is likely to seriously complicate or hamper some computer crime prosecutions. Any attempt to value these types of assets is best left as a matter to be considered during the sentencing process. I would suggest, however, that corporations move quickly to identify through corporate records the developmental or replacement costs of their valuable computer software assets.

The current criminal law and its judicial interpretation for the search and seizure of evidence is incompatible with the current and future organization and storage of information in an electronic form in a distributed data processing environment. Records used by a company in the ordinary course of business may not exist within its business premises but be resident in numerous data banks spread over a very wide area. Often what we think of as a record does not even exist until the program has called various pieces of data together to create the record. From a legal search point of view, there could well be a problem with the standards of particularity of the locations to be searched, and from an evidential point, the

[Translation]

Le temps-machine partagé crée des problèmes propres puisqu'il y a alors mélange de données informatisées. En effet, lorsqu'il s'agit de feuilles, on peut faire un tri matériel, alors qu'il est très difficile d'éviter la sortie de données confidentielles non mentionnées dans l'autorisation puisque la seule façon de s'assurer que l'on a obtenu toutes les données pertinentes, c'est d'examiner tout le système. En outre, les obligations de tenue de dossier et de divulgation que l'on trouve dans les lois fédérales et provinciales doivent être modernisées, par exemple l'article 355 du Code criminel.

L'interception légale. Il n'est pas certain que la transmission de données entre un ordinateur et ses terminaux, entre deux terminaux, ou entre deux systèmes informatiques, soit considérée comme une communication privée au sens des lois actuelles. Par conséquent, cela pose un sérieux problème de preuve qu'il faut régler afin de permettre l'utilisation de mesures efficaces pour les enquêtes sur des crimes informatiques.

Le droit criminel actuel du Canada a les dispositions qu'il faut pour déterminer les infractions que constituent les crimes informatiques, lorsqu'il s'agit de biens tangibles. Toutefois, le rassemblement et la présentation des preuves de ces infractions et d'autres aussi posent certains problèmes. Le droit criminel traite mal des incidents concernant des biens intangibles, comme l'information ou les données informatisées, parce que l'information n'est pas considérée comme un bien ni comme quoi que ce soit qui soit défini en droit criminel.

Le simple fait de conférer le statut de bien ou de propriété aux données ou à l'information ne permettra pas nécessairement les poursuites en vertu des articles portant sur le vol ou la fraude si l'on était obligé de donner une interprétation légale de ce que signifie prendre, copier, traduire ou convertir quelque chose qui demeure toujours à la disposition du propriétaire original. Cela soulèvera également au procès le problème de leur évaluation. L'évaluation que l'on fait des données ou des programmes afin de déterminer en vertu de quel article pénal il est préférable de porter les accusations, risque de compliquer sérieusement sinon d'empêcher toute poursuite pour des crimes informatiques. Toute tentative en vue d'évaluer ce genre de bien ne devrait être faite au mieux qu'au moment de déterminer la sentence. Je suggérerais quand même aux sociétés de se dépêcher d'évaluer, grâce à leurs dossiers, les frais de mise au point et de remplacement de leurs précieux logiciels.

Le droit criminel courant et l'interprétation qu'ont fait les tribunaux de ces dispositions sur la perquisition et la saisie de preuve sont incompatibles avec la façon dont est et sera emmagasinée l'information automatisée dans un réseau de traitement et de distribution des données. Les pièces dont se sert une entreprise pour ses affaires courantes peuvent très bien ne pas se trouver dans les bureaux mêmes, mais dans diverses banques de données réparties sur un très vaste territoire. Souvent ce que l'on peut imaginer comme un dossier n'existe même pas tant que le programme visant à rassembler diverses données n'est pas établi pour le créer de toutes pièces. Légalement parlant, dans une perquisition, on doit tenir

[Texte]

record generated may be inadmissible because it was made in the course of an investigation.

The intention of Parliament in implementing the privacy legislation is unclear as it relates to communications between computers. Additionally, because of the technology involved, it becomes much more difficult, if not impossible, to isolate and examine only that information which is subject to an inquiry. Due to the international nature of computer accessibility and the current high volumes of trans-border data flow, it is important to evaluate the effect of new legislation on our present treaties and agreements that relate to extradition and commission evidence. Every effort should be made to ensure that there are sufficient legal mechanisms available to bring a computer crime perpetrator to court and be able to obtain the necessary evidence to support a conviction.

• 1635

The RCMP do not feel the creation or amending of criminal law is the only alternative to the problems associated with computer abuse. We support development of industry standards of due care, the development of moral and ethical conduct in relation to computer use, and the utilization of the civil process to seek redress.

Additionally, we perceive that some aspects of computer abuse are best addressed in other forms of legislation, such as the Copyright Act or provincial legislation dealing with contracts and torts. We also perceive that public awareness and education is required in this area, and we will continue to expend effort in this area. However, we support the view that amendments are required to the Criminal Code that will define the bounds of acceptable behaviour in relation to computers in our modern society and provide criminal sanctions when those bounds are exceeded. While amendments to the Criminal Code may provide solutions to some of the identified problems in relation to computer abuse, it is imperative that the impact of that legislation be examined in relation to valuation, jurisdiction, evidence, search and seizure, and our international treaties and agreements.

The RCMP respectfully recommends the following actions be taken in relation to criminal law on computer abuse: first, the creation of offences of taking computerized information or data without authority, using a computer in an unlawful manner, or obtaining any unauthorized service from a computer. The offence, while falling under part seven, should not be included within the general theft provisions due to the anticipated problems associated with copying data and determining the value of the occurrence.

Second, the expanding of the provisions of Section 387 of the Criminal Code to include computerized information as something that can be willfully damaged, including the provisions that it can be altered. To avoid the problem of

[Traduction]

compte des normes particulières aux divers endroits à fouiller, et du point de vue de la preuve, le dossier ainsi monté peut être inadmissible parce qu'il a été créé en cours d'enquête.

L'intention qu'a voulu manifester le Parlement en adoptant la Loi sur la protection de la vie privée n'est pas très claire à propos des communications entre ordinateurs. De plus, étant donné la technologie en cause, il devient beaucoup plus difficile, voire impossible, d'isoler et d'examiner les seules données faisant l'objet d'une enquête. Comme l'accès aux ordinateurs est souvent international et que le débit des données franchissant les frontières est extrêmement élevé en ce moment, il importe d'apprécier l'effet des nouvelles lois sur nos traités actuels d'extradition et de preuve. On devrait tout faire pour s'assurer qu'il existe suffisamment de mécanismes légaux pour pouvoir amener jusqu'en cour l'auteur d'un crime informatique et réussir à rassembler les preuves voulues pour aboutir à une condamnation.

La G.R.C. ne croit pas que la modification du droit criminel ou la création d'une nouvelle loi soient les seules façons de régler les problèmes liés aux fraudes informatiques. La G.R.C. favorise l'établissement de normes de précaution pour l'industrie, la mise au point d'un code d'éthique pour l'usage des ordinateurs et l'utilisation d'une procédure civile pour obtenir réparation.

En outre, nous croyons que certains aspects des fraudes informatiques devraient être traités par d'autres types de lois comme la Loi sur le droit d'auteur ou les lois provinciales portant sur les contrats et les délits. Nous croyons également qu'il faut sensibiliser le public, ce à quoi nous allons continuer de nous efforcer. Toutefois, nous sommes d'accord avec ceux qui croient nécessaire d'amender le Code criminel afin de définir les limites de ce qu'est un comportement acceptable en informatique dans notre société moderne et de prévoir des peines en droit criminel quand ces limites sont dépassées. L'amendement du Code criminel apportera peut-être des solutions à certains des problèmes cités à propos des fraudes informatiques, mais il est impérieux que l'effet de cet amendement sur l'évaluation, la juridiction, la preuve, la perquisition et la saisie, ainsi que sur nos ententes et traités internationaux soit bien examiné.

La G.R.C. recommande en toute déférence que les modifications suivantes soient apportées au droit criminel en ce qui concerne les fraudes informatiques: premièrement, qu'on crée de nouvelles infractions que constituerait le fait de prendre sans autorisation des données ou des renseignements informatisés, le fait d'utiliser un ordinateur de façon illégale ou de tirer un service non autorisé d'un ordinateur. Même si ces infractions se retrouveraient dans la partie VII, elles ne devraient pas se trouver dans les dispositions générales traitant du vol, à cause des problèmes qu'on peut envisager pour la copie des données et l'évaluation de l'incident.

Deuxièmement, il faudrait élargir la portée des dispositions de l'article 387 du Code criminel afin d'y ajouter l'information informatisée comme quelque chose qui peut être volontairement détérioré, y compris les dispositions portant qu'un bien

[Text]

valuation, Section 388.(1) should be deemed not to apply to the damage or destruction of computerized information.

Thirdly, that the powers of search and seizure under the Criminal Code as they relate to information stored in a computer system be reviewed.

Fourth, that the privacy provisions of the Criminal Code be examined as it relates to communications between computers. If it is determined that Section 178.(1) applies, then guidelines should be provided in keeping with current technology to satisfy the public interest in terms of privacy, and at the same time facilitate the collection of evidence.

Fifth, that the federal acts and treaties relating to international investigations and extraditions be examined in relation to proposed criminal law amendments.

Sixth, legislation with respect to documentary evidence requires examination and amendment to clarify admissibility of computer-generated documents in criminal proceedings.

While no specifics such as wording or definitions are being offered at this point, the RCMP will provide such assistance as may be necessary in the development of the criminal law and the associated investigational procedures required to combat computer abuse.

Thank you, Madam Chairman.

Le président: Merci, monsieur Allen.

C'est maintenant à mon collègue, M. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Madam Chairman, I wonder, do we start with our first witness first, or do we start with the last one first, or does it make any difference?

The Chairman: It does not matter.

Mr. Robinson (Etobicoke—Lakeshore): I do not know whether I have sufficient time. Maybe I will make my questions fairly short, and deal with the first witness first, then go on to the second.

Mr. Hill, is it?

Mr. Hill: Yes.

Mr. Robinson (Etobicoke—Lakeshore): You made quite a lengthy presentation, and I took a few notes. I will be looking forward to taking a further look at the transcript. I think most of this was kind of an overview, but you might be prepared to give us some information, first of all, with regard to this Mr. Clark, who did a Stanford research study of some 1,000 cases?

Mr. Hill: Mr. Parker of Stanford did the...

Mr. Robinson (Etobicoke—Lakeshore): Oh, Parker. Where did I get Clark from? Parker. Would we be able to get the ratio of these cases, and particularly the ratio of the 10 Canadian cases?

[Translation]

peut être altéré et, pour contourner les problèmes d'évaluation, l'article 388 (1) devrait être réputé ne pas s'appliquer au dommage ou à la destruction d'information informatisée.

Troisièmement, les pouvoirs de perquisition et de saisie en vertu du Code criminel devraient être revus pour ce qui concerne l'information emmagasinée dans un système informatique.

Quatrièmement, les dispositions du Code criminel protégeant la vie privée devraient être revues dans l'optique des communications entre ordinateurs. Si l'on décidait que l'article 178.1 s'applique, il faudrait alors établir des lignes de conduite tenant compte de la technologie actuelle afin de protéger la vie privée des gens tout en facilitant la collecte des preuves.

Cinquièmement, les lois fédérales et les traités concernant les enquêtes internationales et les extraditions devraient être revus à la lumière des amendements proposés au Code criminel.

Sixièmement, la Loi traitant de la preuve documentaire doit être revue et amendée de façon à clarifier l'admissibilité des documents informatisés comme preuve, dans les poursuites au criminel.

Même si la G.R.C. ne fournit pour le moment aucune définition ni libellé précis, elle est disposée à apporter toute l'aide nécessaire pour le développement du droit criminel et des procédures d'enquête corollaires dont on a besoin pour combattre la fraude informatique.

Je vous remercie, madame la présidente.

The Chairman: Thank you, Mr. Allen.

My colleague, Mr. Robinson, now has the floor.

M. Robinson (Etobicoke—Lakeshore): Madame la présidente, par quelle série de témoins doit-on commencer? Y a-t-il un ordre à respecter?

Le président: Cela n'a pas d'importance.

M. Robinson (Etobicoke—Lakeshore): Je ne sais pas si j'aurai assez de temps. Je vais essayer de garder mes questions assez courtes et de commencer par le premier témoin.

C'est M. Hill, n'est-ce pas?

M. Hill: Oui.

M. Robinson (Etobicoke—Lakeshore): Vous avez fait un long exposé et j'ai pris des notes. J'ai bien hâte de pouvoir revoir la transcription. Je crois que vous avez surtout voulu nous donner un aperçu, mais vous êtes peut-être disposé à nous donner davantage de renseignements, en commençant par ce M. Clark, qui aurait fait une recherche à Stanford sur quelques 1,000 affaires.

M. Hill: M. Parker, de Stanford, a fait...

M. Robinson (Etobicoke—Lakeshore): Ah, c'est Parker. D'où a bien pu me venir ce nom de Clark? Serait-il possible d'obtenir la proportion de ces affaires, surtout celle des dix affaires canadiennes?

[Texte]

• 1640

[Traduction]

Mr. Hill: I believe Mr. Avison may be able to assist you.

Mr. Avison: Yes, Madam Chairman, we can provide that information.

Mr. Robinson (Etobicoke—Lakeshore): Then you mentioned there were some surveys taken by the Ontario Provincial Police. It seems to me it would be interesting to know the kind of questions asked in that survey, if we could have that made available to us.

Mr. Hill: Yes, I will do so.

Mr. Robinson (Etobicoke—Lakeshore): In regards to it, the indication you gave was that there were 321 responses. I am wondering how many copies of the survey were sent out. Were they sent to all police forces or all detachments? What was the number sent out, and what was the return? I wonder if this is a significant factor, but maybe additional information on this might give that kind of information. In other words, was there really any interest in reporting back to the OPP on their survey?

Mr. Hill: I have enough copies here for each member of the committee. I will introduce them through the clerk, Madam Chairman. It seems to me the survey suggests that 640 corporations and institutions were actually sent the questionnaire, with 321 responses.

Mr. Robinson (Etobicoke—Lakeshore): So that is about 5%.

Mr. Hill: No, it would be 50%.

Mr. Robinson (Etobicoke—Lakeshore): Yes, I should say 50%. Now, that is a very high return on a survey. Was there any compulsion to reply, or was it merely because it was of such specific interest?

Mr. Hill: Mr. Campbell, who I believe was responsible for the survey, would be the best person to address those issues.

Mr. Robinson (Etobicoke—Lakeshore): Mr. Hill, you indicated some of the information might properly fall within civil or criminal jurisdiction, or maybe either one or both. It would seem to me, if it falls within the civil jurisdiction, we are really talking about damages; and if it falls within the criminal jurisdiction, we are talking about crime.

Are you suggesting, if it were just under criminal jurisdiction, there may also be damages awarded by way of restitution or something of this nature, so that you could proceed either under the criminal law or the civil law? Then I am wondering where the onus lies. Is there a heavier onus, in your view, if a case is presented in the criminal law or an action is brought by way of civil proceedings?

Mr. Hill: Let me deal first with the question of the criminal proceedings. At many of our consultations, the question arose as to the redress that would be available under the existing provisions of the Criminal Code. Insofar as damages were concerned, the existing provision in the Criminal Code would enable compensation of non-controversial liquidated damages to be awarded; and this would be enforceable in the civil court.

M. Hill: Je crois que M. Avison va pouvoir vous aider.

M. Avison: Oui, madame la présidente, nous pouvons fournir ces renseignements.

M. Robinson (Etobicoke—Lakeshore): Vous avez également dit que la Sûreté provinciale de l'Ontario avait fait quelques sondages. Il serait intéressant, me semble-t-il, de savoir quel genre de questions ont été posées dans ces sondages. Peut-être pourrions-nous obtenir copies des questionnaires.

M. Hill: Oui, je m'en occupe.

M. Robinson (Etobicoke—Lakeshore): Il semble qu'on ait reçu 321 questionnaires remplis. Je voudrais savoir combien d'exemplaires ont été envoyés. En a-t-on envoyé à toutes les polices ou à tous les détachements? Combien de questionnaires ont été envoyés et combien ont été renvoyés remplis? J'ignore si cela a de l'importance, mais je voudrais obtenir davantage de renseignements de ce genre. Autrement dit, les gens étaient-ils intéressés à participer au sondage de la sûreté de l'Ontario?

M. Hill: J'ai ici suffisamment d'exemplaires pour tous les membres du Comité. Je vais les remettre au greffier. Il semble que 640 sociétés et institutions aient reçu le questionnaire; et 321 auraient répondu.

M. Robinson (Etobicoke—Lakeshore): C'est donc un taux de réponse de 5 p. 100.

M. Hill: Non, plutôt de 50 p. 100.

M. Robinson (Etobicoke—Lakeshore): En effet. C'est un taux de réponse très élevé pour un sondage. Les gens étaient-ils obligés de répondre ou l'ont-ils fait par pur intérêt?

M. Hill: M. Campbell, le responsable du sondage, je crois, serait mieux placé pour vous répondre.

M. Robinson (Etobicoke—Lakeshore): Monsieur Hill, vous avez dit que certains renseignements seraient de juridiction civile, d'autres de juridiction criminelle, et certains des deux à la fois. S'il s'agit de juridiction civile, il est plutôt question de dommage, tandis que, s'il s'agit de juridiction criminelle, il s'agit d'un crime.

Voulez-vous dire que même si c'était uniquement de juridiction criminelle, on pourrait obtenir des dommages et intérêts sous forme de restitution ou de quelque chose de ce genre, si bien qu'on aurait le choix de poursuivre soit en vertu du droit criminel, soit en vertu du droit civil? Je voudrais savoir où se trouve le fardeau. À votre avis, le fardeau de la preuve est-il plus lourd lorsqu'un procès est intenté au criminel plutôt qu'au civil?

M. Hill: Je vais commencer par répondre à votre question sur les procédures au criminel. Lors de nombreuses séances de consultations, on s'est demandé quel recours serait possible en vertu des dispositions actuelles du Code criminel. Pour ce qui est des dommages, la disposition du Code criminel permettrait l'octroi d'une compensation pour des dommages non controversés et évalués. Ce jugement pourrait être exécuté par un

[Text]

You could walk across from the criminal court to the civil courtroom and enforce it. However, based on the Zilansi case, it is very much in doubt, if the damages were unliquidated and controversial, as to whether or not the criminal court would be entitled to embark on that exercise.

Therefore, one aspect of the problem we have discerned in our consultations is that companies prefer to use other techniques for dealing with the problem than reporting the abuse as a crime. Included in those techniques is to arrange a settlement with the employee, if it is an employee; and alternatively, there is some evidence that insurance claims may or may not be the subject of a settlement.

• 1645

Dealing with the question of on whom the onus lies, as far as the civil-criminal remedies go, I think it is very difficult to say that there is an onus. An onus can be placed by legislation. It is largely a question of whether a particular victim considers it best to go to the criminal court or goes the civil route. On the other hand, under the statutory monopolies as they now exist, the criminal sanction is so minimal and inconsequential that there is a disincentive to use it if it is available in any particular case.

Mr. Robinson (Etobicoke—Lakeshore): It seems to me that the victim should not be in a position to be able to decide the forum he is going to use, either criminal or civil. Surely you are not suggesting that?

Mr. Hill: No, we are not suggesting that. What we are saying is that unless the matter comes to the attention of the law enforcement agencies, then it is difficult to see how a prosecution could be initiated.

Mr. Robinson (Etobicoke—Lakeshore): Let me put it this way. Do you see the victim taking civil action but also giving the information to the police so that a criminal charge could be brought as well?

Mr. Hill: Certainly, if the conduct was the subject of criminal sanctions. In fact, what we are trying to do is to create a legislative scheme that encourages reporting over and above any civil redress that may be available.

Mr. Robinson (Etobicoke—Lakeshore): Would you suggest in this procedure that the action be taken first in the criminal side, where there is a much higher onus, and, if successful there, proceed by way of damages under civil litigation?

Mr. Hill: Well, the position in Canada now is that there is no real requirement for criminal proceedings to be brought first, as I understand jurisprudence. Invariably, if the victim is interested in prosecuting the wrongdoer, it is likely he will choose the criminal route first but there is no legal requirement for him to do so.

Mr. Robinson (Etobicoke—Lakeshore): I suppose there would be no incentive to proceed with the civil consequences or suing civilly for damages if in fact the perpetrator of the crime

[Translation]

tribunal civil. Vous n'auriez qu'à traverser le couloir, passant du tribunal criminel au tribunal civil pour faire exécuter le jugement du premier. Toutefois, si l'on se fonde sur l'affaire Zelenski, il est fort peu probable que, pour des dommages controversés et pas évalués, le tribunal criminel ait le droit de faire cette démarche.

Par conséquent, l'un des aspects du problème que nous avons réussi à cerner en faisant des consultations, c'est que les sociétés préfèrent utiliser d'autres moyens pour régler le problème plutôt que de porter plainte pour fraude. Parmi ces méthodes on trouve la conclusion d'un règlement avec l'employé, s'il s'agit d'un employé. Il se pourrait qu'un tel règlement soit l'objet de réclamations auprès des compagnies d'assurance.

Pour ce qui est de savoir sur qui repose la responsabilité de choisir entre les recours civils et criminels, je crois qu'on peut difficilement affirmer qu'il existe une obligation quelconque. La loi pourrait en imposer une. C'est surtout la victime qui décide si elle juge préférable d'intenter des poursuites au civil ou de porter plainte au criminel. En revanche, en vertu des dispositions régissant les monopoles légaux d'exportation, les sanctions prévues au criminel sont si infimes et insignifiantes qu'on préfère ne pas y avoir recours même si c'est possible.

M. Robinson (Etobicoke—Lakeshore): Il me semble que la victime ne devrait pas être en mesure de choisir la juridiction criminelle ou civile. Ce n'est pas ce que vous avez voulu dire, n'est-ce pas?

M. Hill: Non. Mais si l'affaire n'est pas portée à l'attention de ceux qui doivent appliquer la loi, comment voulez-vous que des accusations soient portées?

M. Robinson (Etobicoke—Lakeshore): Serait-il possible que la victime intente une poursuite au civil et communique en même temps les renseignements à la police afin que des accusations soient aussi portées au criminel?

M. Hill: Certainement, si les actions sont passibles de peines au criminel. De fait, nous voudrions une loi qui inciterait les gens à porter plainte, en plus de se pourvoir au civil, si possible.

M. Robinson (Etobicoke—Lakeshore): Préférez-vous alors que les accusations soient portées au criminel d'abord, parce que la responsabilité est plus grande, et s'il y a condamnation, ensuite réclamer des dommages intérêts au civil?

M. Hill: À l'heure actuelle au Canada rien n'oblige quelqu'un à intenter des procédures criminelles d'abord, si j'en juge par la jurisprudence. Si la victime veut poursuivre le malfaiteur, elle commencera presque toujours par le criminel, mais légalement rien ne l'exige.

M. Robinson (Etobicoke—Lakeshore): Je suppose qu'il n'est pas très intéressant de poursuivre au civil, en dommages et intérêts, l'auteur d'un crime qui est sans le sou. Le seul

[Texte]

is impecunious. Obviously, the only incentive would be to stop him from doing it again by using criminal procedures.

Mr. Hill: Yes, but there is also another pattern we have discerned. A lot of victims regard criminal sanction as a public forum in which disclosure of security measures, confidential information and matters of this sort are paraded in open view and this has always, notwithstanding the example you have given, constituted factors which are taken into account.

Mr. Robinson (Etobicoke—Lakeshore): Did I understand from your remarks that you consider there should be some amendments to the Criminal Code which would cover this situation? In other words, what you are suggesting is that it would be criminal legislation primarily; but I would suggest to you that any federal statute has criminal consequences insofar as penalty is concerned. All federal statutes are, in effect, criminal in nature.

Mr. Hill: Well, I suppose, technically, you are correct. They could be justified under peace, order and good government and they could be justified under essential inferences. Copyright is a federal constitutional power in any event, so it would not require criminal jurisdiction to impose penalties.

Mr. Robinson (Etobicoke—Lakeshore): In other words, unless you created new pieces of legislation and could proceed under present legislation, or even if you did create new federal pieces of legislation, they would all have criminal consequences.

Mr. Hill: They would have criminal sanctions.

Mr. Robinson (Etobicoke—Lakeshore): But I assumed as well you were thinking there might be some overlapping of jurisdiction with the provinces.

Mr. Hill: Yes, that is so.

Mr. Robinson (Etobicoke—Lakeshore): Is this where the recommendation would be that in order to have one jurisdiction dealing with the matter, there should be amendments to the Criminal Code rather than the setting up of provincial and/or federal legislation?

• 1650

Mr. Hill: No, we have not come to any view on how the shared responsibility might be legislated. That is one of the primary reasons for having Professor Hammond undertake the study. You could have a situation in which a provincial statute declares something to be a trade secret and provides remedies or relief. At the same time you could have a criminal statute which would be within the federal jurisdiction and which says if you steal a trade secret which is defined in terms of what the provincial statute says it is . . . operating at the same time.

Mr. Robinson (Etobicoke—Lakeshore): Could I suggest to you that so far there have not been any meetings with the provinces, or your counterparts in the provinces, on this very problem?

Mr. Hill: I think a meeting is scheduled for either April 7 or 8 to discuss this.

[Traduction]

moyen alors de l'empêcher de recommencer, c'est d'intenter une procédure au criminel.

M. Hill: Oui, mais nous avons pu déceler une autre façon de faire. Bien des victimes considèrent les procédures au criminel comme une audience publique où on doit divulguer ses mesures de sécurité, ses renseignements confidentiels, et autres questions de ce genre. Or, outre l'exemple que vous avez donné, ces facteurs sont toujours pris en considération.

M. Robinson (Etobicoke—Lakeshore): Si je vous ai bien compris, vous croyez que le Code criminel devrait être amendé de façon à prévoir cette situation, n'est-ce pas? Autrement dit, vous suggérez qu'il y ait d'abord et avant tout une loi au criminel. Je dois vous faire remarquer que toute loi fédérale pénale a les mêmes conséquences que le Code criminel. Toutes les lois fédérales sont effectivement de nature criminelle.

M. Hill: Techniquement parlant, vous avez raison. On pourrait justifier leur nécessité par les principes de paix, d'ordre et de bon gouvernement, en plaçant leur caractère essentiel. Le droit d'auteur est de toute façon un pouvoir constitutionnel du gouvernement fédéral; on pourrait donc avoir une loi pénale qui ne serait pas nécessairement criminelle.

M. Robinson (Etobicoke—Lakeshore): Autrement dit, que vous créiez de toutes nouvelles lois fédérales ou que vous vous serviez de la loi actuelle, tout cela aurait des conséquences au criminel.

M. Hill: Ce serait les mêmes peines qu'au criminel.

M. Robinson (Etobicoke—Lakeshore): J'ai présumé que pour vous il y aurait chevauchement sur la juridiction des provinces.

M. Hill: C'est exact.

M. Robinson (Etobicoke—Lakeshore): Est-ce la raison pour laquelle vous recommandez qu'on amende le Code criminel au lieu d'adopter une nouvelle loi provinciale ou fédérale, de façon à assurer qu'une seule juridiction traite de ces causes?

M. Hill: Non, nous ne savons pas encore comment transcrire dans les lois ce partage de compétences. C'est d'ailleurs une des principales raisons pour laquelle le professeur Hammond a entrepris cette étude. Ainsi, il pourrait arriver qu'aux termes d'une loi provinciale, telle ou telle chose deviendrait un secret commercial avec toutes les mesures législatives que cela entraîne, alors qu'en même temps une loi pénale, donc de juridiction fédérale, fixerait des sanctions en cas de vol de secret commercial tel que défini par des lois provinciales.

M. Robinson (Etobicoke—Lakeshore): Comment se fait-il que jusqu'à présent, il n'y ait pas eu de réunions entre le gouvernement fédéral et les gouvernements provinciaux à ce sujet?

M. Hill: Une réunion est justement prévue le 7 ou le 8 avril.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): I think the committee would certainly be interested in knowing what the provinces think about co-operating with the federal government approach in this, and also whether they would be prepared to delegate any legislative powers they have provincially to the federal government to deal with computer crime.

Mr. Hill: May I just make two comments? The first is that when the initial impact of the McLaughlin case came out, there was correspondence between the Minister of Justice and provincial attorneys general dealing with the problem. At that time I think the minister was Mr. Chrétien. It was his view that both our levels of government would have an interest, and there was clearly a view that there would be co-operation from the provincial AGs.

I should also indicate that at our consultation in Toronto—the national consultation—I think it was a member of the Alberta Law Reform Commission who indicated that he had reasonable grounds for believing that certainly his commission and the province from which he came would be interested in looking at Professor Hammond's report from a provincial perspective. So we do not foresee any difficulty in getting both levels of government to co-operate in this area.

Mr. Robinson (Etobicoke—Lakeshore): So it might properly be a matter for a federal-provincial conference at some stage, along with other matters.

Mr. Hill: Yes, that is correct.

Mr. Robinson (Etobicoke—Lakeshore): You mentioned that Mr. MacBain, the Parliamentary Secretary, had provided some information. I think it would be helpful to the committee if we—I suppose the chairman could obtain this for us.

Mr. Hill: I was referring to Mr. MacBain's speech as reflected in the House of Commons debates on the bill of . . .

The Chairman: On the bill.

Mr. Hill: It is in the record.

Mr. Robinson (Etobicoke—Lakeshore): Maybe the clerk could arrange to see that we get copies of everything that took place at that time.

You mentioned Professor Hammond and the various aspects of his report and the research that he is doing, and I believe you also recommend that he might be a person we would want to have appear before the committee. Would you consider him as one of the people we should have fairly early in our work, or one later on, to wrap up? At what stage do you think he would be most helpful to the committee?

Mr. Hill: Certainly as shortly as possible after our presentation. He has indicated his willingness, if he is required to come to Ottawa.

Mr. Robinson (Etobicoke—Lakeshore): I think those are all the questions I want to ask you at the moment, because I want to go on with our other witness, and time is very short.

Mr. Hill: I would just like to clarify one point. When I say "our presentation", I mean after the committee has heard from Mr. Avison, Mr. Piragoff, and Mrs. Gilhooly.

[Translation]

M. Robinson (Etobicoke—Lakeshore): Le Comité devrait connaître la position des provinces en ce qui concerne leur coopération éventuelle avec le gouvernement fédéral à ce sujet; nous voudrions également savoir si les autorités provinciales seraient disposées à déléguer au gouvernement fédéral les pouvoirs législatifs dont elles disposent pour que l'on puisse s'attaquer aux infractions en informatique.

M. Hill: Le ministre fédéral de la Justice et les procureurs généraux des provinces ont procédé à un échange de correspondance concernant l'affaire McLaughlin. C'est M. Chrétien qui était titulaire à l'époque. Il était d'avis que les deux niveaux de gouvernement devraient s'intéresser à cette question et qu'il y aurait donc une coopération entre son ministère et les procureurs généraux des provinces.

Par ailleurs, lors de nos consultations à Toronto, un membre de la Commission de la réforme juridique de l'Alberta, a dit qu'à son avis la Commission à laquelle il appartient et la province de l'Alberta ne manqueraient pas d'étudier le rapport du professeur Hammond du point de vue provincial. La coopération entre les deux niveaux de gouvernement ne devrait donc pas poser de problème.

M. Robinson (Etobicoke—Lakeshore): Cette question pourrait donc être inscrite éventuellement à l'ordre du jour d'une conférence fédérale-provinciale.

M. Hill: Oui.

M. Robinson (Etobicoke—Lakeshore): Je pense qu'il serait utile que le président du Comité obtienne à notre intention les renseignements fournis par M. MacBain, le secrétaire parlementaire.

M. Hill: Je parlais de l'allocution de M. MacBain à la Chambre des communes lors du débat sur le projet de loi . . .

Le président: C'est ce projet de loi-ci.

M. Hill: C'est exact.

M. Robinson (Etobicoke—Lakeshore): Le greffier aura l'obligeance de nous faire parvenir tous les documents afférents.

Vous avez mentionné le rapport et les travaux du professeur Hammond en ajoutant qu'il serait bon qu'il comparaisse devant le Comité. À votre avis, devrions-nous l'entendre au début ou à la fin de nos travaux?

M. Hill: Il devrait suivre aussi rapidement que possible notre intervention, il a d'ailleurs fait savoir qu'il était tout disposé à venir à Ottawa.

M. Robinson (Etobicoke—Lakeshore): C'est tout ce que j'avais à vous demander pour l'instant.

M. Hill: Je voudrais simplement préciser un point. Quand je dis après notre intervention, j'entends après celle de M. Avison, M. Piragoff et M^{me} Gilhooly.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): Mr. Allan, you gave a long dissertation here, and I note on page 1 where you indicated:

· For the most part poor application of security measures have been the cause of complaint and has resulted in otherwise appropriate security being compromised.

Mr. Robinson (Etobicoke—Lakeshore): Tell me what you mean by this application of security measures. Are there security measures available and which should be taken but are not being taken, apart from the reporting to the police, this sort of thing?

• 1655

Supt Allen: Yes, sir, that is correct. In the few cases we have had we have found that the security measures in place, had they been properly applied, would have prevented the complaint. For example, you would find that an access code designed to guard the security of the computer system might be posted beside the terminal because the people in the corporation could not remember what the access code was. This type of measure, generally speaking, is what has caused the majority of cases we have found.

Mr. Robinson (Etobicoke—Lakeshore): Why do you tend to put the onus on the victim? Do you not feel that the police have an obligation to be in the front of these things, or is it because of the nature of this particular crime?

Supt Allen: With us having found that the majority of the cases are where there has been poor internal security control, aside from the police force promoting crime prevention, from a law enforcement standpoint there is very little we can do within the corporate structure, and a lot of the responsibility must return to the corporation for them to address internally as a security problem.

Mr. Robinson (Etobicoke—Lakeshore): What I am really thinking of is the kind of situation where the police monitor the radios of truck drivers, and so on, for various reasons. It just seems to me that with the sophistication of technology today there should be somehow you can be at least up with the game, if not ahead of the game, in being able to monitor computer systems, computer setups, to know if someone is interfering with a computer.

Supt Allen: Our experience has been that we have been interpreting the computer transmissions as private transmissions for purposes of our criminal investigations, and in once case we had difficulty in obtaining an authorization under the Code to intercept a communication for the simple reason that there were multiple transmissions or a packet of information being sent down the line which would have meant that we would have had to intercept other transmissions from other users of the system. Therefore, we have had difficulty doing that and so I do not think we could legally monitor the lines to see that there was proper usage, and assist corporations that way, without a legislative amendment.

Mr. Robinson (Etobicoke—Lakeshore): I see. What form of legislative amendment are you thinking of, something like the wire-tap legislation?

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Je relève le passage suivant à la page 1 de l'exposé de M. Allan:

C'est le plus souvent une mauvaise application des mesures de sécurité qui est à l'origine des ennuis, compromettant ainsi des mesures de sécurité bonnes en elles-mêmes.

M. Robinson (Etobicoke—Lakeshore): Qu'entendez-vous par une mauvaise application des mesures de sécurité? Voulez-vous dire que, à part le fait de signaler le cas à la police, on omet d'appliquer certaines mesures de sécurité en vigueur?

Sdt Allen: Oui, c'est exact. Nous avons pu constater en effet dans les cas qui nous ont été signalés qu'il n'y aurait pas eu de problème si les mesures de sécurité en vigueur avaient été appliquées. Ainsi le code d'accès, qui est censé assurer la sécurité de l'ordinateur, était affiché à côté du terminal parce que les travailleurs de la société n'arrivaient pas à s'en souvenir. Dans la plupart des cas, c'est ce genre d'incident qui est à l'origine des ennuis.

M. Robinson (Etobicoke—Lakeshore): Vous avez, semble-t-il, tendance à blâmer les victimes. Est-ce à cause du caractère de ces infractions?

Sdt Allen: Bien que la police cherche dans toute la mesure du possible à réprimer le crime, nous ne pouvons pas faire grand-chose lorsque la majorité des infractions sont imputables à des carences de la sécurité intérieure des sociétés; il incombe donc à ces sociétés de mettre bon ordre dans leur sécurité.

M. Robinson (Etobicoke—Lakeshore): Je sais que la police peut surveiller les radios des camionneurs pour diverses raisons. Vu la technologie poussée dont vous disposez, vous devriez en principe pouvoir surveiller également les ordinateurs pour déterminer si quelque chose de frauduleux se passe.

Sdt Allen: Les transmissions sur ordinateur sont assimilées à des transmissions privées aux fins de nos enquêtes pénales; ainsi dans un cas nous avons eu du mal à obtenir l'autorisation de capter une communication pour la bonne raison que celle-ci faisait partie d'un ensemble de communications transmises sur une ligne, ce qui nous aurait obligés à capter les transmissions d'autres usagers. Donc à moins que la loi ne soit modifiée en ce sens, je ne pense pas que nous puissions légalement surveiller les lignes pour assurer qu'il n'y ait pas infraction.

M. Robinson (Etobicoke—Lakeshore): Je vois. Faudrait-il une loi analogue à celle relative aux écoutes téléphoniques?

[Text]

Supt Allen: Certainly, to intercept specific transmissions we would need some direction that would spell out the fact that the privacy provisions apply to computer transmissions, but I suppose we would also have to look at some form of legislation similar to the telecommunications which allows certain companies, such as Bell, to monitor its lines to see that the usage is in conformity with the laws.

Mr. Robinson (Etobicoke—Lakeshore): The same with Hydro; they do the same thing. There have been people tapping into lines for years, and who eventually get caught because they have a way of seeking them out and finding out who is doing it, by testing the lines.

I notice that on page 2 you indicate a major area of concern, this unauthorized use from within the organization. You indicate that this does not constitute a criminal offence. I do not follow that. It seems to me that if it is a criminal offence outside the organization, it should properly be a criminal offence within the organization.

Supt Allen: Here I think we are referring to the individual who has legitimate access to the computer and to the computer system, and he is using it to run his own tallies with respect to football games, or he is having printouts. Quite often you will see people going around with the computer printout of their name repeated several thousand times on the page. It is this type of usage that some of the corporations are concerned with, from within the organization. That access is legitimate, but it is misuse of the equipment.

Mr. Robinson (Etobicoke—Lakeshore): But you do not consider that as criminal in nature.

Supt Allen: No, I would not, sir.

• 1700

Mr. Robinson (Etobicoke—Lakeshore): Well, supposing the employer came along to you and said: I want to charge my employee with doing this kind of thing. He appears before a justice of the peace and gives him some information—do you think that a charge would be laid?

Supt Allen: I do not think so, sir. An analogy would be the secretary who types a letter to her sister-in-law on the typewriter. She would have a legitimate access to the typewriter, but what she is doing with it is on corporate time would certainly not be in the best interests of the corporation. But to be criminal—I do not think we would look at it as a criminal offence.

Mr. Robinson (Etobicoke—Lakeshore): Well, I mean if there was intent and if it was done wilfully and so on, why would it not be considered as criminal in nature?

Supt Allen: I must say, sir, I have not addressed myself to that particular issue beyond coming to the conclusion that it would not be grounds for the police to conduct an investigation when an employee has misused the equipment of the firm.

Mr. Robinson (Etobicoke—Lakeshore): Well there would be no point then in considering civil consequences because you would have to prove damages and there is probably no damage to the employer.

[Translation]

Sdt Allen: Pour nous permettre de capter les transmissions, il faudrait préciser que les transmissions informatisées sont en principe secrètes; on pourrait également envisager une loi analogue à celle sur les télécommunications, laquelle permet à des sociétés comme Bell de surveiller ses lignes pour assurer qu'il n'y ait pas d'entorse à la loi.

M. Robinson (Etobicoke—Lakeshore): Les sociétés d'électricité peuvent faire la même chose. Elles arrivent ainsi à dépister les personnes qui ont réussi à rester brancher sur le réseau pendant des années.

Vous parlez également à la page 2 du problème causé par l'utilisation non autorisée au sein d'une entreprise, utilisation qui d'après vous ne constitue pas une infraction. Je ne vois pas pourquoi ce qui est une infraction à l'extérieur ne le serait pas au sein d'une organisation.

Sdt Allen: Il s'agit en l'occurrence de personnes qui peuvent légitimement se servir des ordinateurs, mais qui s'en servent pour leur usage privé. C'est cet usage parfois excessif que les sociétés cherchent à freiner. Il s'agit donc de personnes qui tout en ayant droit de se servir des ordinateurs, s'en servent pour leur propre usage.

M. Robinson (Etobicoke—Lakeshore): A votre avis, cela ne constitue pas un crime.

Sdt Allen: Non.

M. Robinson (Etobicoke—Lakeshore): Si un patron intentait des poursuites contre ses employés devant un juge de paix, pensez-vous qu'il obtiendrait une inculpation?

M. Allen: Je ne le pense pas. Prenons le cas d'une secrétaire qui se sert de sa machine à écrire pour écrire des lettres personnelles. Elle a le droit de se servir de la machine à écrire, mais elle gaspille ainsi le temps, qui en pratique appartient à la société. Il ne s'agit néanmoins pas d'un acte criminel.

M. Robinson (Etobicoke—Lakeshore): Si c'était fait intentionnellement, pourquoi ne serait-ce pas un acte criminel.

Sdt Allen: Tout ce que je puis vous dire, c'est qu'à mon avis la police ne pourrait pas en pareil cas ouvrir une enquête.

M. Robinson (Etobicoke—Lakeshore): Comme l'employeur en l'occurrence ne pourrait pas prétendre avoir subi de dommage, on ne pourrait donc pas tenter des poursuites civiles.

[Texte]

Supt Allen: Unless a person could show that the use of time itself on the equipment had some value that could be determined by the firm.

Mr. Robinson (Etobicoke—Lakeshore): Can you tell us, what are some of the necessary measures that you feel the industry should be using to protect itself against this type of activity where the employee is using up computer time unauthorized, if not unlawfully?

Supt Allen: I would say, sir, that a good internal security program would have to include the education of employees with respect to the use of the equipment and the need to guard the confidentiality of access codes and of other information that is in the system.

Mr. Robinson (Etobicoke—Lakeshore): On page 4, at the end of the first paragraph—at just about the end of it you say:

—one of the motivating factors in the refusal to invoke the criminal process is the belief that the laws are inadequate to effectively deal with this type of criminality.

Is this generally so? Do the computer people, or anybody who has a computer, really feel the laws are totally inadequate? I mean we have laws regarding theft and many, many sections of the Criminal Code that might be right on point in many cases.

Supt Allen: Yes, that is true. I have had personal contact where I have been told that. In one particular case, which I referred to earlier, in which we were unable to obtain an authorization to intercept a computer communication, the victim was very upset that the police could really do nothing to assist him and this was one of the views expressed by him. I know on other occasions in talking to firms, they have chosen to take the internal route, for whatever reason, as opposed to reporting it to the police because of the expediency of it in asking the employee to simply pay back what he has taken and be gone and not get involved in the process which may or may not deal with the crime itself.

Mr. Robinson (Etobicoke—Lakeshore): I see that our time is virtually up and I am only on page 4 of your 15 pages. I do hope we will be able to have you back so that I can continue questioning. So maybe I can end it with just this last question which refers to the second last paragraph on page 4, where you indicate that there were no reported incidents of industrial espionage known about by the RCMP in Canada. I can assume that even though they had not been reported, there may be some. You are not suggesting that there had not been any?

Supt Allen: No, as a matter of fact, there are. It might not be called industrial espionage; we have had a couple of cases in which individuals have accessed statistical information which has been compiled, and the results of studies—and have taken that information for their own use. I suppose one might say that it was a form of espionage—the pirating of certain information that a corporation has put together. In another case certain scientific results were taken by an individual who was an employee of the company. He took them off for his own personal use.

[Traduction]

Sdt Allen: À moins que la firme n'arrive à prouver que l'utilisation de l'ordinateur pendant un certain temps représente en soi une valeur.

M. Robinson (Etobicoke—Lakeshore): Qu'est-ce que les entreprises pourraient faire pour empêcher les employés d'utiliser les ordinateurs pour leur propre usage?

Sdt Allen: Un programme de sécurité interne devrait comprendre, entre autres, un cours offert aux employés sur l'utilisation des ordinateurs et la nécessité de veiller au secret des codes d'accès et de l'ensemble des données se trouvant dans le système.

M. Robinson (Etobicoke—Lakeshore): Vous dites ce qui suit à la page 4 fin du dernier paragraphe:

... une des raisons pour lesquelles on se refuse à tenter des poursuites pénales est la conviction que les lois ne sont pas en mesure de régler ce genre d'infraction.

Est-ce bien le cas pensez-vous? Nous avons toute une série de lois traitant du vol, ainsi que différents articles du Code criminel, qui pourraient fort bien s'appliquer à ce genre d'infraction.

Sdt Allen: J'ai entendu ce point de vue exprimé à plusieurs reprises. Ainsi dans une affaire que j'ai déjà citée lorsque nous n'avons pas obtenu l'autorisation de capter une communication, la personne lésée s'est exprimée en ce sens, constatant que la police n'était pas à même de lui venir en aide. Dans d'autres cas, les firmes ont préféré régler l'affaire directement avec l'employé fautif, qui était renvoyé après avoir été obligé de rembourser la firme. En l'occurrence ces sociétés ont préféré agir ainsi plutôt que de passer par la police.

M. Robinson (Etobicoke—Lakeshore): Je ne suis qu'à la page 4 de votre rapport, qui en comporte 15 alors, et mon temps de parole est pratiquement épuisé. J'espère que vous pourrez revenir parce que j'ai encore d'autres questions à vous poser. Vous dites dans l'avant-dernier paragraphe, à la page 4, que la Gendarmerie royale n'avait pas connaissance de cas d'espionnage industriel au Canada. Mais même si vous n'en avez pas connaissance, cela ne signifie pas nécessairement que l'espionnage industriel n'existe pas chez nous.

Sdt Allen: En effet, ce sont des cas qui arrivent, même s'il ne s'agit pas d'espionnage industriel à proprement parler. Ainsi nous avons suivi deux affaires dans lesquelles des personnes avaient relevé des données statistiques et des résultats d'étude dans un ordinateur pour s'en servir à leur propre usage. On pourrait qualifier cela d'espionnage dans un certain sens. Nous connaissons un autre cas où un employé a sorti des résultats scientifiques d'un ordinateur également pour son propre usage.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): Thank you very much, Mr. Allen.

The Chairman: Merci, Mr. Robinson.

Maybe just for practical—I could ask for Mr. Hill. You were referring to a list of experts whom you consulted . . .

• 1705

Did these people submit the brief to you or do you have any record of these witnesses appearing before your committee? Because my feeling is that we have some researchers working for this committee and not to repeat, really, in this committee exactly what has been done by your committee. I trust what you have done already, certainly well done, and I would rather start from where you left. Is this material available, or do you have a summary or . . .

Mr. Hill: We have the actual briefs, the briefs submitted by the 17 of the group in Toronto. We have the actual briefs which our committee can make available to the committee.

The Chairman: Thank you so much. I think the members of the committee would appreciate it and our researcher could—this would help also in inviting these people at a later date if we feel that we need to question or have more information.

And my question for Mr. Avison is that RCMP—my question is, since we do not have a lot of reported crimes, have we investigated or do we have any data giving us the unreported details? Meaning, have we tested by poll or Delphi method what is happening in fact instead of—of course we have the reported cases, but do we have all the cases that might have been reported? Do we have a notion of the size? There is the article that was submitted by Mr. Hill saying that billions of dollars are at stake. Well, we have a problem that we have to deal with.

I was wondering if either RCMP or the statistics branch has done something to see to what extent this problem is . . . well, there is a problem. But the size of it, we really are in the dark as far as I am concerned.

Supt Allen: Madam Chairman, from our point of view we do not even have all the statistics of the various police forces in Canada. So we are just speaking from our own point of view and its very limited statistical data. And no, we have not done any surveys.

Mr. Avison: But I think it is fair to say that Mr. Allen did mention that from different conferences, congresses and so on one gets an informal indication of what is going on. There appears to be quite a lot of computer abuse going on.

On the basis of the review of cases gathered in Stanford, it is possible to describe them under various headings and get some estimate of the likelihood of different sorts of crime appearing. And I can produce that, obviously.

The other thing that I thought the committee might like to consider—I could bring along a small computer to show the types of security which are in place in a large, well-organized and RCMP- approved installation. I cannot demonstrate any breach of security but I can at least demonstrate what happens

[Translation]

M. Robinson (Etobicoke—Lakeshore): Merci, commissaire Allen.

Le président: Merci, monsieur Robinson.

Je voudrais poser une question à M. Hill. Vous avez mentionné une liste d'experts que vous consultez.

Ces personnes vous ont-elles soumis un mémoire et auriez-vous un compte rendu de leur comparution devant votre comité? Ce serait en effet une perte de temps si nos chercheurs allaient refaire le travail déjà effectué par les vôtres. Il vaudrait mieux coordonner les travaux de nos deux comités. Auriez-vous des comptes rendus de vos travaux?

M. Hill: Nous avons les mémoires, présentés par les 17 du groupe de Toronto, nous pourrions vous les communiquer.

Le président: Ce serait très utile aussi bien pour les membres du Comité que pour nos chercheurs, et cela pourrait également nous servir si nous décidions d'inviter ces personnes ou si nous avions des questions à leur poser.

Puisque le nombre d'infractions signalées à la police n'est pas important, possédons-nous au moins des détails concernant le reste de ces infractions? A-t-on fait des enquêtes pour déterminer l'ampleur du problème en dehors des cas signalés à la police? Selon l'article de M. Hill, ces infractions porteraient sur des milliards de dollars. C'est donc un vrai problème.

Je voudrais donc savoir si la Gendarmerie royale ou la direction des statistiques a cherché à déterminer l'ampleur du problème, dont nous savons très peu pour l'instant.

Sdt Allen: Madame le président, nous ne disposons même pas des statistiques des diverses polices du Canada. Ce que nous avons dit étant basé uniquement sur les données, très restreintes, dont nous disposons. Nous n'avons pas par ailleurs fait enquête.

M. Avison: M. Allen a souligné néanmoins que l'utilisation illicite des ordinateurs est un gros problème d'après ce qu'on en dit à l'occasion de divers congrès.

D'après le relevé de ce type de cas effectués à Stanford, on peut les cataloguer sous diverses rubriques et essayer de prévoir leur incidence. Je pourrais si vous voulez vous communiquer ce document.

Je pourrais également, si vous le voulez, amener un petit ordinateur pour vous montrer le genre de mesures de sécurité mises en place dans un gros organisme, dont l'installation a été approuvée par la Gendarmerie. Je pourrais ainsi vous montrer ce qui arrive lorsqu'on essaie de circonvenir les mesures de sécurité. Je pense que dix minutes de ce genre de démonstra-

[Texte]

when you try to breach security. And perhaps 10 minutes of looking at this might be worth half an hour of chit-chat.

The Chairman: Yes. Thank you.

My assumption is this, that as far as statistics are concerned we are well aware that—having been with us also, General, before—that we do not have, in other areas, perfect statistics with regard to any crime. So I understand it is a problem. We are probably—we have a good record if we look at the international scene, from various conferences I have attended. But nevertheless, we do not really have all the basic data we would need. And I was just suggesting that maybe at a later stage we would appreciate, certainly, more accuracy with the methods that we have. Like I am suggesting Delphi method, or there could be some polls to discover which area is certainly more sensitive.

Because of course there is the area related to the software, but also related to the scientific application of computer science. Because we tend to put the commercial application and the scientific one in the same bag, but my impression is that the value of computer information is certainly on the scientific side very valuable but this is, to my knowledge, not very much researched and looked into and the commercial side is certainly more evident. That is why I just say to myself that we are still a little bit in the dark.

• 1710

I was wondering if the RCMP has checked government security with regard to the data bank, if they were consulted, and if they have worked with various departments to establish a security control for government data banks.

Supt Allen: Yes, Madam Chairman, the RCMP has a unit which provides assistance and advice to other government departments. I am not qualified to speak on the technical aspects, but we would certainly be pleased to put someone at the disposition of the committee to ask any questions in the area with respect to the security application and its use by other government departments.

The Chairman: Do you have any reported cases of infraction with regard to the government data bank?

Supt Allen: No, I do not have one, Madam Chairman.

Mr. Avison: I have one.

The Chairman: You have one?

Mr. Avison: Yes. Some public employees in an eastern province were using a federal computer to set up a tax advisory and business calculation business as a private enterprise. So while it is not actually an invasion of the government data bank, it is clearly a misappropriation of federal resources. That is one of the 10 cases which were picked up in the Stanford data base.

Supt Allen: Something similar, Madam Chairman—we have another one where a program was developed on government time and then ultimately modified for what we believe was going to be personal use.

[Traduction]

tion vous en apprendraient plus qu'une demi-heure de bavardage.

Le président: Certainement, merci.

Ce qui est certain, c'est qu'il n'existe pas de statistique parfaite, quelle que soit l'infraction. Nous ne sommes d'ailleurs pas si mal placés par rapport à ce qui se passe dans d'autres pays, mais il est certain que nous n'avons pas suffisamment de données à ce sujet. Il faudrait également mettre au point des méthodes plus précises; c'est pourquoi j'avais proposé la méthode Delphi pour mettre la situation au clair.

Il y a également la question du logiciel et l'utilisation de l'informatique à des fins scientifiques. Nous avons souvent tendance à confondre l'utilisation scientifique et commerciale de l'informatique, alors que l'utilisation de l'informatique à des fins scientifiques a une importance énorme. Or j'ai l'impression que l'on a peut-être sous-estimé cet aspect pour insister davantage sur l'aspect commercial. Toute la lumière n'a pas encore été faite sur cette question.

Je voudrais savoir si la Gendarmerie vérifie la sécurité des banques de données du gouvernement et des divers ministères.

Sdt Allen: La Gendarmerie possède en effet une unité chargée d'aider et de conseiller les divers ministères à ce sujet. Je ne suis pas moi-même spécialiste dans ce domaine, mais si vous le voulez nous pouvons mettre un spécialiste à votre disposition pour répondre aux questions relatives à la sécurité des banques de données des ministères.

Le président: Vous a-t-on signalé des cas d'infraction dans des banques de données du gouvernement?

Sdt Allen: Non, pas à ma connaissance, madame le président.

M. Avison: Moi, j'en ai entendu.

Le président: Ah oui.

M. Avison: Oui. Des fonctionnaires travaillant dans une province de l'est utilisaient un ordinateur du gouvernement fédéral pour une entreprise privée qu'ils avaient créée dans le domaine des conseils fiscaux et des calculs d'entreprises. Donc même si la banque de données du gouvernement n'a pas fait l'objet d'une fraude, il y a quand même eu utilisation des biens du gouvernement à des fins illicites. C'est d'ailleurs un des dix cas cités dans le dossier de Stanford.

Sdt Allen: On nous a également signalé le cas d'un programme élaboré pendant les heures de travail à l'aide des ordinateurs du gouvernement, programme utilisé pour l'usage privé des personnes en question.

[Text]

The Chairman: It is just to demonstrate that I think we are exactly in the same position as private industry and that we have to deal with the problem for our own purpose as well as the public and the private sector.

I would like to go back, maybe to ask Mr. Hill on the project and the multiple approach they have developed, when would you be ready to table a bill? I mean, do they have a draft? At what stage are they? What kind of timeframe are we talking about? Are we talking about being ready for next fall, or being ready in two months' time after consultation with the provinces, for instance?

Mr. Hill: Madam Chairman, the proposal which Mr. Piragoff will deal with reflects the first half of our work. That I think could be ready for the spring; in fact, I gather that is being contemplated. There are a few refinements that have to be done, and we hope to meet with the draftsman next week to complete that exercise. As far as the multi-vehicle approach, that would be more to the fall, and that is our mandate.

The Chairman: So that means that Mr. Piragoff is dealing with the criminal law approach; I mean just with the Criminal Code and the criminal aspects of the problem. And when we deal with the other legislation . . . the patent law, the Official Secrets Act, the Evidence Act, and all the others—would we have wait for that at a later date?

Mr. Hill: It is likely that the report of Professor Hammond and the consultations with the provinces will go through into the summer. It is unlikely that legislation will be before the fall on the other half.

The Chairman: Well, it is a bit to organize our own work, because I have the feeling we could be maybe complementary to your action. But certainly, as I say, I do not want to start over everything that has been done; and also, in a practical approach, our committee will have to at a later date study the proposal of the Department of Justice. Of course, maybe for part of it I would rather study it from a bill than study the overall problem.

• 1715

Of course, with no specific proposal on the table . . . So I will discuss that with my colleagues on the committee and see how we could . . . And then also proceed with a two-step approach, as you did, which is a very practical way of dealing with it.

Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): I just want to ask one question of Mr. Hill, and also from Mr. Allen. Mr. Hill, do you know what the Law Reform Commission is doing with regard to any of the areas of computer crime? If they are doing something, it might be helpful for us to have them appear before the committee.

Mr. Hill: I do know that they are currently reviewing the mischief provisions of the Criminal Code, Part IX. Prior to embarking upon our work, we did interview two members of the commission staff, and my recollection is—and Ms Gilhooly can correct me—it did not seem to us as though they were

[Translation]

Le président: Tout ceci montre que le gouvernement se trouve dans une situation analogue au secteur privé et que nous allons devoir essayer de régler ce problème aussi bien pour le secteur public que privé.

M. Hill pourrait-il nous dire où en sont ses travaux et s'il compte déposer prochainement un projet de loi. Avez-vous un calendrier? Quand comptez-vous pouvoir prendre des mesures pratiques?

M. Hill: La proposition dont M. Piragoff vous parlera représente la première partie de notre travail. En principe nous devrions être prêts pour le printemps. Il y a encore quelques retouches à faire et nous devons justement rencontrer le rédacteur la semaine prochaine pour terminer ce travail. La réponse globale par contre ne sera prête qu'à l'automne prochain.

Le président: M. Piragoff s'occupe donc des aspects criminels de la question et du Code criminel. Pour ce qui est de l'incidence de ces infractions au plan de la Loi sur les brevets, de la Loi sur les secrets officiels, de la Loi sur la preuve au Canada etc., il faudra donc encore attendre.

M. Hill: Les consultations avec les provinces se poursuivront durant l'été. Des lois sur l'autre moitié du problème ne seront donc pas prêtes avant l'automne.

Le président: Je vous ai posé toutes ces questions en vue de nos propres travaux, lesquels sont plus ou moins complémentaires aux vôtres. Il faudrait dans toute la mesure du possible ne pas faire ce qui a déjà été fait ailleurs. Le Comité devra d'ailleurs éventuellement étudier les propositions du ministère de la Justice. Mais il faudra commencer par examiner les dispositions du projet de loi plutôt que de prendre le problème dans son ensemble.

Bien entendu, il n'y a aucune proposition précise de déposée . . . j'en discuterai donc avec mes collègues du Comité afin de voir si nous pouvons également adopter cette procédure en deux étapes, comme vous l'avez fait, car cela me paraît une solution très pratique.

Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): J'aimerais poser une question à M. Hill, et également à M. Allen. Monsieur Hill, êtes-vous au courant de ce que la Commission de réforme du droit fait en ce qui a trait aux infractions en informatique? Si cet organisme a pris des mesures quelconques, il sera peut-être utile que nous fassions témoigner certains de ses membres.

M. Hill: La Commission étudie présentement les dispositions relatives aux méfaits de la partie IX du Code criminel. De plus, avant de lancer nos travaux, nous avons interviewé deux membres de la Commission, et je crois me souvenir que l'organisme n'envisageait pas d'étudier ce problème de la

[Texte]

going to deal with this problem in the way we are dealing with it, and that was why we were given the mandate.

Mr. Robinson (Etobicoke—Lakeshore): I see.

Mr. Allen, you have given us some recommendations, but they are not in any drafted form, merely ideas for recommendations for change in the present law under the Criminal Code. Maybe some of it would not necessarily be under the Criminal Code but under other statutes. Do you have any draft legislation, draft sections, draft suggestions or proposals?

Supt Allen: No, we do not have anything formulated at present. We have been consulted with respect to some of the papers that are being submitted on this, but I do not have specific sections and recommendations . . .

Mr. Robinson (Etobicoke—Lakeshore): Will you be drafting something of this nature?—because it might be helpful to the committee to have something like this to look at from the point of view of the RCMP.

Supt Allen: No, we had not intended to embark on anything of that nature. If it would be helpful, I suppose we could prepare something for you.

Mr. Hill: Madam Chairman, I could indicate that in a general way the RCMP have provided us with inputs on what is contemplated to be . . .

The Chairman: You are working in consultation.

Mr. Hill: Yes.

Mr. Robinson (Etobicoke—Lakeshore): I realize that I cannot get draft legislation from you, but maybe I can get some from him. That is why I did not ask you, Mr. Hill.

The Chairman: My impression, my dear colleague, is that we do not ask the police to draft the legislation, even though I have a lot of respect for the RCMP people.

Mr. Robinson (Etobicoke—Lakeshore): They have draftsmen, too.

Mr. Hill: Madam Chairman, before you conclude I just realized that I have another, more current, article—it is 1982—dealing with this whole question of assessing computer crime incidence and statistics and the cost of infractions as a whole. I wonder if we might table this?

The Chairman: *Merci.* Yes.

Mr. Hill: Thank you.

The Chairman: I would like to thank the witnesses for appearing on such short notice and for the RCMP preparing a good summary of their views on the subject-matter. We might be in a position to be in touch again after we go through the literature, the report and all the documents you have tabled today. We have other meetings scheduled next week. We are due to make a preliminary report to the main committee on March 30 so after we have our instructions from the main committee, of course, we will be more in a position to know

[Traduction]

même façon que nous; c'est pourquoi c'est à nous qu'on a confié ce mandat. Si je me suis trompé ici, M. Gilhooly pourra me corriger.

M. Robinson (Etobicoke—Lakeshore): Je vois.

Monsieur Allen, vous nous avez fait certaines recommandations, mais pas sous forme écrite. Il s'agit plutôt de modifications possibles à apporter au Code criminel actuel. De plus, certains de ces changements ne relèveraient pas nécessairement du Code criminel, mais du droit statutaire. Cependant, avez-vous déjà rédigé des modifications de lois ou d'articles, ou encore des propositions?

Sdt Allen: Non, nous n'avons rien rédigé jusqu'à maintenant. On nous a bien consultés au sujet de certains documents se rapportant à la question, mais nous n'avons pas mis sur papier d'article précis ou de recommandation . . .

M. Robinson (Etobicoke—Lakeshore): Allez-vous en rédiger? Il serait peut-être utile au Comité de disposer de quelque chose de ce genre à consulter, et je songe ici aux points de vue de la GRC.

Sdt Allen: Non, nous n'avons pas l'intention de nous lancer dans ce genre d'entreprise. Je suppose toutefois qu'il serait utile de vous préparer quelque chose.

M. Hill: Madame le président, en général, la GRC nous a fourni des renseignements sur ce que l'on entrevoit être . . .

Le président: Vous travaillez en collaboration.

M. Hill: Oui.

M. Robinson (Etobicoke—Lakeshore): Je me rends compte que je ne puis obtenir de projet de loi de vous, mais peut-être sera-ce possible de lui. C'est pour cela que je ne vous ai pas interrogé, monsieur Hill.

Le président: Mon cher collègue, je crois vraiment que l'on ne demande pas à la police de rédiger des projets de loi, malgré tout le respect que je porte aux membres de la GRC.

M. Robinson (Etobicoke—Lakeshore): Elle compte des rédacteurs, elle aussi.

M. Hill: Madame le président, avant que vous ne terminiez, je me rends compte que j'ai un autre article, datant celui-là de 1982 et portant sur l'évaluation de l'incidence des crimes commis par ordinateur; il comprend également les statistiques et le coût des infractions. Pouvons-nous faire déposer ces documents?

Le président: *Merci.* Oui.

M. Hill: *Merci.*

Le président: J'aimerais remercier les témoins d'avoir comparu à si brève échéance, ainsi que la GRC d'avoir préparé un bon résumé de ses idées là-dessus. Une fois que nous aurons étudié tous les documents que vous avez déposés aujourd'hui, ainsi que le rapport, il se peut que nous entrions à nouveau en contact avec vous. Par ailleurs, il y a d'autres séances de prévues pour la semaine prochaine. Nous devons présenter un rapport provisoire au comité principal le 30 mars, après quoi, une fois que nous aurons reçu les instructions du comité

[Text]

how the committee will proceed at a later date because we understand that in two weeks we do not expect to be able to cover and come up with decent recommendations since you have worked on this with a good team for quite a while.

I would like also to say that on Wednesday, March 23, at 3.30 p.m., we will have Mr. Jim Finch, of Jim Finch and Associates from Toronto, who will appear as a witness. I just thank you and hope to see you again. I apologize to Miss . . . ; it is not because we do not have an interest in the legal aspect and the legislation in the U.S., but our researcher will be in touch with you also to get the pieces of legislation that we might consider from other countries like the U.S., which has an approach that might be similar to ours. From your statement, I realize they have legislated, but the result does not seem to be there. So I would not like to take the same approach, at least to be pragmatic and have some results on the kind of action we will recommend.

• 1720

Thank you so much *Mesdames, messieurs*. The meeting is adjourned.

[Translation]

principal, nous serons davantage en mesure de savoir comment agir plus tard, car nous ne nous attendons pas à arriver à des recommandations convenables d'ici deux semaines seulement, compte tenu du fait que vous avez fait travailler une bonne équipe sur les vôtres pendant une bonne période.

Par ailleurs, je vous rappelle que le mercredi 23 mars à 15h30, nous entendrons les témoignages de M. Jim Finch, de *Jim Finch and Associates*, de Toronto. Je vous remercie et espère vous revoir. Je m'excuse auprès de mademoiselle. Ce n'est pas que nous ne nous intéressions pas à l'aspect juridique ainsi qu'à la législation des États-Unis, mais notre chercheur vous contactera afin que vous puissiez obtenir les lois d'autres pays, que nous aimerions peut-être étudier. Je songe ici à celle de États-Unis, dont la démarche se rapproche assez de la nôtre. D'après ce que vous en avez dit, je crois que ces pays ont déjà adopté une loi, sans toutefois qu'on en ait senti les conséquences. Je tiens donc à ce que nous ne prenions pas la même voie, mais que nous soyons plutôt pratiques afin d'obtenir des résultats.

Merci beaucoup, mesdames et messieurs. La séance est levée.



If undelivered, return COVER ONLY to
Canadian Government Printing Office
Supply and Services Canada
45 Sacre-Coeur Boulevard
Hull, Quebec, Canada K1A 0S7

En cas de non livraison
retourner cette COUVERTURE SEULEMENT à
Imprimerie du gouvernement canadien
Approvisionnement et Services Canada
45 boulevard Sacre Cœur
Hull, Québec, Canada K1A 0S7

WITNESSES—TÉMOINS

From the Department of Justice:

Mr. Norman Hill, Project Chief, Theft and Fraud Project;
Mr. Neville Avison, Chief, Research & Statistics.

Du Ministère de la Justice:

M. Norman Hill, Chef de projet, Projet vol et fraude;
M. Neville Avison, Chef, Recherche et statistiques.

From the Royal Canadian Mounted Police:

Superintendent George W. Allen, Commercial Crimes
Branch.

De la Gendarmerie Royale du Canada:

Surintendant George W. Allen, Section délits commerciaux.

3 HOUSE OF COMMONS

Issue No. 2

Wednesday, March 23, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 2

Le mercredi 23 mars 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Order of Reference

CONCERNANT:

Ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

DESIGNATED ALTERNATES/SUBSTITUTS DÉSI-
GNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, MARCH 23, 1983

(4)

[Text]

The Sub-committee on computer crime met this day at 3:35 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Designated Alternate Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From Cerberus Computer Security Inc: Mr. James H. Finch and Mr. Collin C. Rous, Toronto.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15th, 1983, Issue No. 1*)

The Chairman presented the First Report of the Sub-Committee to the Standing Committee on Justice and Legal Affairs which was read as follows:

In accordance with the Order of Reference of Tuesday, March 1st, 1983, your Sub-committee has commenced consideration of the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime and requests leave to resume consideration of its Order of Reference after the Easter recess.

On motion of Mr. Robinson (*Etobicoke—Lakeshore*), the first report of the Sub-committee on computer crime was concurred in.

Ordered,—That the Chairman report to the Standing Committee on Justice and Legal Affairs.

Mr. Robinson (*Etobicoke—Lakeshore*) assumed the Chair.

Mr. Finch and Mr. Rous made a statement and answered questions.

At 5:29 o'clock p.m. the Committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 23 MARS 1983

(4)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h 35, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, chercheuse, Service de la recherche, Bibliothèque du Parlement.

Témoins: De Cerberus Computer Security Inc: MM. James H. Finch et Collin C. Rous, Toronto.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbaux du mardi 15 mars 1983, fascicule no. 1*)

Le président présente le premier rapport du Sous-comité au Comité permanent de la justice et des questions juridiques qui se lit comme suit:

Conformément à son Ordre de renvoi du mardi 1^{er} mars 1983, votre Sous-comité a commencé l'étude de l'objet du projet de loi C-667, Loi modifiant le Code Criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs et demande la permission de poursuivre l'étude de son Ordre de renvoi après l'ajournement de Pâques.

Sur motion de M. Robinson (*Etobicoke—Lakeshore*), le premier rapport du Sous-comité sur les infractions relatives aux ordinateurs est adopté.

Il est ordonné,—Que le président fasse rapport au Comité permanent de la justice et des questions juridiques.

M. Robinson (*Etobicoke—Lakeshore*) assume la présidence.

M. Finch et M. Rous font une déclaration et répondent aux questions.

A 17h 29, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Comité

Pierre de Champlain

Clerk of the Committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Wednesday, March 23, 1983

• 1534

Le président: À l'ordre!

• 1535

Before introducing our witness this afternoon, I would like to consult with my colleagues on this committee to send the subcommittee's first report to the main committee about the proceedings of our subcommittee, because I feel we had a very short timeframe, and having looked at the amount of work that has to be done, I would send that report back to the main committee, which would be that pursuant to its order of reference of Tuesday, March 1, 1983, your subcommittee has commenced consideration of the subject-matter of Bill C-667, an Act to Amend the Criminal Code and the Canada Evidence Act in respect of computer crime, and requests leave to resume consideration of its order of reference after the Easter recess.

If you agree with that—because I think our calendar will certainly be longer, and since we had to report before the end of March and next week we will be entering into April—so I just thought I would submit that.

An hon. Member: Agreed.

The Chairman: So I will introduce our two witnesses from Cerberus Computer Security Inc., Mr. James Finch—welcome, Mr. Finch—and Mr. Colin C. Rous.

I would like to apologize to the witnesses. I will have to leave you in the hands of my colleagues. I have three commitments at the same time. I have to give a speech in the House and also attend the main committee on Justice, so I would like to ask if Mr. Robinson would act as chairman of this... I will read your comments in the proceedings of this subcommittee. I would like to thank you also for agreeing to appear before us on such short notice. Thank you so much.

Mr. Beatty: You recognize, Mrs. Chairman, that this means you cannot ask questions. It is reserved for the members of the committee to put questions.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): As the chairman of this committee *pro tem*, I will give myself special consideration. Even though the committee does not officially have a vice-chairman, I suppose I am probably acting in that position at the moment.

We are very pleased indeed to have our witnesses with us.

Mr. Finch, do you have a statement you wish to make first? And what about your colleague; does he have a statement as well?

Mr. Jim Finch (James Finch and Associates and Cerberus Computer Security Inc.): I have a statement, Mr. Chairman,

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mercredi 23 mars 1983

The Chairman: Order please!

Avant de vous présenter notre témoin de cet après-midi, j'aimerais consulter mes collègues membres du Comité au sujet de l'envoi au comité plénier du rapport du Sous-comité. Je pense que les délais qui nous ont été imposés sont très courts et, étant donné le travail qui reste à faire, j'aimerais qu'on renvoie le rapport au comité. Ce rapport se lit comme suit: Conformément à son ordre de renvoi du mardi 1^{er} mars 1983, votre Sous-comité a commencé l'étude de l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs et demande la permission de poursuivre l'étude de son Ordre de renvoi après l'ajournement de Pâques.

Si vous êtes d'accord... parce que nous aurons besoin de délais supplémentaires... nous devons déposer notre rapport avant la fin du mois de mars, mais le mois d'avril commence dès la semaine prochaine... C'est pourquoi je pensais qu'il serait bon que nous envoyions ce rapport.

Une voix: D'accord.

Le président: Je vais maintenant vous présenter nos deux témoins, qui représentent la *Cerberus Computer Security Inc.* Il s'agit de MM. James Finch et Colin C. Rous. Bonjour.

J'aimerais m'excuser auprès des témoins. Je dois malheureusement m'absenter, et vous laisser avec mes collègues. J'ai trois engagements, pour la même heure. Je dois prononcer un discours à la Chambre et je dois également assister à la réunion du Comité de la justice. Je demanderai donc à M. Robinson de présider cette... Je lirai les commentaires que vous ferez dans le procès-verbal de la réunion du Sous-comité. Je tiens également à vous remercier d'avoir accepté de venir comparaître devant nous, malgré le très court préavis qui vous a été donné.

M. Beatty: Vous n'ignorez pas, madame le président, que cela signifie que vous ne pourrez pas poser de questions. Ce privilège est réservé aux membres du Comité.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À titre de président par intérim du Comité, je m'acconderai des concessions spéciales. Même si le Comité n'a pas de vice-président officiel, je suppose que c'est ce poste que je suis en train de remplir à l'heure actuelle.

Nous sommes ravis d'accueillir nos témoins.

Monsieur Finch, avez-vous une déclaration préliminaire à nous faire? Et votre collègue?

M. Jim Finch (James Finch et associés et Cerberus Computer Security Inc.): Monsieur le président, j'ai une

[Texte]

that I think can start the ball rolling, and then we invite you certainly to ask all questions that you would like.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you have copies of your statement available to us?

Mr. Finch: Because of the very short notice, I do not have copies. Probably the record will be the best copy. But I am organized in some fashion, so hopefully we will not cover the ground in too many ways.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Fine. We will let you make your comments, and then Mr. Beatty and I will have a few questions for you.

Mr. Finch: Thank you.

By way of introduction, I would like to explain that I am a computer security analyst, or consultant, and my main occupation is preventing computer abuse. So I am coming to you today—the position I will be taking today is the use of legislation in helping to prevent computer crime.

I am a technician, and Colin Rous, my associate, is an extremely qualified systems programmer, which means that probably between us we understand all the technicalities of how computer crimes may be accomplished.

I invite you as I talk, and later, to interrupt, and if there is information you would like to follow on later at another time, we would be glad to come back to you with the necessary formal information.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): May I suggest that you propose to tell us how one can commit computer crime at the present time?

Mr. Finch: Yes, we can—I do not propose to tell you that. I propose to explain to you why the Criminal Code should be applied; why computer abuse and computer crime should be subject to the Criminal Code, from a business point of view.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): The reason why I say that, Mr. Finch, is because this is an open meeting, it is not an in camera session, and anything you are putting on the record is public knowledge. If you were telling people how they could commit computer crime, by way of explaining it to this committee, this is really not the time or place to do that.

Mr. Finch: No, no. I did not . . .

[Traduction]

déclaration à lire, et je propose de mettre les choses en marche, après quoi vous pourrez nous poser toutes vos questions.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Avez-vous des copies de votre déclaration que vous pourriez nous remettre?

M. Finch: Compte tenu du bref préavis que nous avons eu, je n'ai pas eu le temps de faire faire des copies. Le mieux, serait sans doute que vous vous reportiez au procès-verbal. Mais je suis plus ou moins organisé, et j'essaierai de ne pas trop m'éparpiller.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Nous vous laisserons vous expliquer, après quoi M. Beatty et moi-même vous poseront des questions.

M. Finch: Merci.

En guise d'introduction, j'aimerais vous dire que je suis analyste en sécurité pour les ordinateurs, ou expert-conseil, si vous préférez, et je m'intéresse tout particulièrement à empêcher l'abus des ordinateurs. Je vais vous parler aujourd'hui de l'utilisation des lois pour aider à empêcher les infractions contre les droits de propriété relatifs aux ordinateurs.

Je suis technicien et Colin Rous, mon associé, est un programmeur de systèmes très qualifié, ce qui signifie que nous pouvons à deux comprendre probablement tous les aspects techniques des infractions contre les droits de propriété relatifs aux ordinateurs qui peuvent être commises.

Je vous invite à intervenir et même à m'interrompre, et s'il y a des renseignements sur lesquels vous aimeriez revenir plus tard, je serais heureux de vous fournir des données supplémentaires.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Puis-je me permettre de vous demander de nous expliquer comment on peut commettre une infraction contre les droits de propriété relatifs aux ordinateurs?

M. Finch: Oui, on peut vous le dire, mais je n'en ai pas l'intention. Ce que je me propose de faire, c'est vous expliquer pourquoi il faut recourir au Code criminel, pourquoi l'abus des ordinateurs et les infractions contre les droits de propriété relatifs aux ordinateurs devraient être couverts par le Code criminel.

• 1540

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Si je dis cela, monsieur Finch, c'est parce que notre réunion ne se déroule pas à huis clos. Par conséquent, tout ce que vous direz sera du ressort public, dès l'apparition du procès-verbal. Si vous aviez compté expliquer aux gens comment il est possible de commettre des infractions contre les droits de propriété relatives aux ordinateurs, je voulais tout simplement vous avertir que le moment n'est peut-être pas opportun pour faire pareille chose.

M. Finch: Non. Je ne . . .

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): In some other forum it could probably be presented at a later time.

Mr. Finch: Yes, Mr. Chairman, I did not propose to do that. I do not like to give publicity to that aspect of the subject.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): By the same token, if you have some suggestion to make as to how you can demonstrate to the committee at an in camera session this very thing, which would be helpful to the committee in coming to some conclusions, we would be more than happy to hear from you at a later date.

Mr. Finch: We would be pleased to discuss the type of demonstration that might be appreciated, that you might like to see, I think.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right, fine. Carry on, Mr. Finch.

Mr. Finch: What I will do is go through a number of points. I am going to speak to you very much as many of my clients speak to me, I am going to speak to you as though I were a businessman, an owner of a business with a computer, rather than as a consultant to that.

I am very concerned that in relation to effective legislation—and I believe effective legislation is a key to setting standards in the prevention of computer abuse—in many cases much of our thinking comes from the academic world and sometimes from government viewpoints. And while educational institutions and the government have some of the largest computers in the country, most of the computers are in industry, so it is industry that stands to suffer the greatest losses. Government and education are not the real world of business. That does not mean that there is not a real world of government or a real world of education, but in those areas policies and attitudes towards computers may be compromised by politics, or for very practical reasons in a particular situation. In industry and business, however, the situation is much more straightforward.

As a businessman, any copying or modifying of data from my corporate computer system is a very serious abuse and should be dealt with under the Criminal Code. As an independent company operator, my business is heavily automated and my computer contains information vital to ongoing operations, to future planning and to the particular way in which we define and manage our products and services. Any tampering with, or divulging or loss of, some or all of this information, especially to a competitor, could quickly cause my business to deteriorate or even collapse, could take away a competitive advantage and techniques that have taken years to develop, and could give my competitors information that would adversely affect me.

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ce genre d'explications pourraient vraisemblablement être fournies plus tard, dans le cadre d'une autre tribune.

M. Finch: En effet, monsieur le président, je n'avais aucunement l'intention de faire cela. Je ne voudrais pas faire de la publicité au sujet de cet aspect de la question.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais si vous envisagiez démontrer les différents mécanismes au comité lors d'une séance à huis clos, ce qui serait fort utile dans le cadre de nos travaux, nous serions ravis de vous accueillir de nouveau parmi nous.

M. Finch: Il nous ferait grand plaisir de discuter avec vous du genre de démonstrations que vous aimeriez peut-être voir et qui pourraient vous être utiles.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Poursuivez, monsieur Finch.

M. Finch: Je vais passer en revue un certain nombre de points. Je vais vous parler de la même façon que nombre de mes clients s'adressent à moi; je vais vous parler en tant qu'homme d'affaires et en tant que propriétaire d'une société qui a un ordinateur, plutôt qu'à titre d'expert-conseil en la matière.

Ce qui me préoccupe en matière de législation... et je pense que la mise en place d'une législation efficace est la clé de l'établissement de normes pour la prévention des infractions contre les droits de propriété relatifs aux ordinateurs... Dans de nombreux cas, ce que nous pensons découle du monde universitaire et parfois même des opinions énoncées par le gouvernement. Et, bien que les institutions éducatives et le gouvernement possèdent des ordinateurs qui comptent parmi les plus gros du pays, la plupart des ordinateurs appartiennent à l'industrie, et c'est donc l'industrie qui risque de perdre le plus. Le gouvernement et le domaine de l'éducation ne font pas partie du vrai monde des affaires. Cela ne veut pas dire qu'il n'existe pas de vrai monde du gouvernement ou de vrai monde de l'éducation, mais dans ces domaines les politiques et les attitudes qui se rapportent aux ordinateurs peuvent être compromises par la politique ou, dans certains cas bien précis, par des raisons des plus pratiques. Or, dans le monde de l'industrie et des affaires, la situation est beaucoup plus claire, beaucoup plus directe.

En tant qu'homme d'affaires, toute reproduction ou toute modification de données contenues dans mon système informatique constitue un abus des plus graves et devrait être couvert par le Code criminel. En tant qu'entrepreneur indépendant, ma boîte est très automatisée et mon ordinateur contient des données qui sont vitales à la poursuite de mes activités, à ma planification et à la façon dont je veux définir et gérer mes produits et mes services. Tout traficage, toute divulgation ou toute perte de tous ou d'une partie de ces renseignements, notamment si c'est un concurrent qui en bénéficie, pourrait rapidement amener la détérioration voire l'effondrement de ma société, éliminer mon avantage concurrentiel et les techniques qu'il m'a fallu des années pour mettre au point, et fournir aux

[Texte]

In these economic times we are a tight, no-nonsense company; we are too busy in a highly competitive marketplace to play games with our computers; we have done well over the years, largely through hard work, and we are not about to accept the loss, or the possibility of loss, of our data lightly. We are not a government department or agency where some, or a great deal of, data is already in the public domain, so we are only concerned with, perhaps, the manner in which it might have been taken or copied. For example, in a government installation it is possible that the information rightfully belongs in the public... but if someone should access it at midnight on a Sunday the issue then seemingly becomes, well, it is not that he could not have had the information, he just did not use the right channels. So what we are dealing with is, did he improperly take the information, and there is less concern that the information was taken.

We are not an educational institution with creative students, where rewards are often given to challenge the students or to recognize that they have abused systems. We are prepared to give incentives to our employees to serve us well and we do want deterrents, to staff and to outsiders alike, to support our belief that monkeying with our computer is wrong.

Civil suits are very costly. They are time-consuming and they are not likely to be satisfying. We want strong deterrents. We want appropriate penalties. We are doing our very best to prevent computer abuse, but we must have legislation to provide a very vital deterrent.

Now, I would like to amplify some of these points, but please interrupt if there is any clarification needed.. Today in society we treat "system-hackers" as heroes. The news media looks for the "hero" who broke into the system. We have attitudes being fostered at schools and universities where the teachers, actually and admittedly, encourage students to break the system. And I do not mean only to break their own systems but, if we look at the case of the Dalton school children in New York a few years back, to break into other systems—even into systems in other countries. There is the well known statement from one of our Ontario universities where, if you can bring the system down, you win a pitcher of beer. Of course, you are asked to explain to the operations staff how you did it. They feel that is a less expensive way of de-bugging a system.

[Traduction]

sociétés qui me font concurrence des données qui, en leurs mains, pourraient me nuire.

Les temps sont durs, et ma société fonctionne sans fioriture; nous sommes trop occupés à travailler sur un marché très concurrentiel pour nous adonner à des jeux avec nos ordinateurs. Nous nous sommes bien débrouillés au fil des ans, mais cela est surtout imputable au dur travail que nous avons fait, et nous ne sommes pas prêts à accepter à la légère toute perte ou tout risque de perte de nos données. Nous ne sommes un ministère ou un organisme gouvernemental où une partie, ou peut-être même une bonne partie des données sont déjà du ressort public; par conséquent, nous ne nous préoccupons peut-être que de la façon dont ces données peuvent nous être prises ou de la façon dont nos méthodes peuvent être copiées. Par exemple, s'il s'agit d'une installation gouvernementale, il est fort possible que les renseignements qui s'y rapportent appartiennent au public... Mais si quelqu'un se pointe à minuit un dimanche, alors les choses sont différentes. Le problème n'est pas qu'il ne devrait pas avoir accès à ces renseignements, mais qu'il n'a pas utilisé les méthodes appropriées pour les obtenir. La question qui importe le plus est de savoir s'il avait ou non le droit de prendre ces renseignements ou s'il s'y est mal pris. On se préoccupe beaucoup moins du fait que les données aient été prises.

Nous ne sommes pas une institution éducative à laquelle affluent des étudiants créatifs, qui offre des récompenses pour encourager les étudiants ou pour reconnaître qu'ils ont abusé des systèmes. Nous sommes prêts à mettre en place des mesures d'encouragement pour que nos employés nous servent bien et nous voulons qu'il y ait des mesures de découragement, qui s'adressent tant au personnel qu'aux gens de l'extérieur, afin qu'il soit bien clair que nous n'accepterons pas que l'on vienne trafiquer notre ordinateur.

Les actions civiles sont très coûteuses. Elles prennent beaucoup de temps et elles ne donnent en général pas de résultats satisfaisants. Nous voulons des mesures dissuasives qui soient efficaces. Nous voulons des pénalités appropriées. Nous faisons de notre mieux pour empêcher l'abus des ordinateurs, mais seules des lois constitueraient des moyens dissuasifs efficaces.

• 1545

Je vais maintenant fournir des explications supplémentaires au sujet des points que je viens de soulever, et je vous invite à m'interrompre si vous avez besoin de quelque éclaircissement. Aujourd'hui, notre société traite les «démolisseurs de systèmes» comme des héros. Les media recherchent le «héros» qui réussit à comprendre le système et à s'en servir. Dans les écoles et les universités il y a des enseignants qui encouragent les étudiants à le faire, et qui le reconnaissent. Et je ne parle pas ici uniquement des systèmes propres aux écoles. Prenez par exemple les étudiants de l'Ecole Dalton, à New York: il y a quelques années, ils ont déchiffré d'autres systèmes, même des systèmes de pays étrangers. Dans l'une des universités de l'Ontario, celui ou celle qui parviendra à déchiffrer le système se fera payer un pichet de bière. Bien sûr, le gagnant sera tenu d'expliquer au personnel comment il a réussi à faire son coup.

[Text]

We have long had problems with employee attitudes in the data processing industry. The data processing employees have shown a strong loyalty to technology as opposed to their employer. And now with hard times where, in some cases, seniority is not a guarantee of employment, I think the loyalty to the technology is even stronger; I think there is more of a tendency and more encouragement for an employee not to recognize, but to take advantage of, his employer.

We are also faced with difficulty in employee screening. Because of human rights legislation, we are not always able to know as well as we would like the character of people we hire. So we feel that the use of the Criminal Code as a deterrent is very important.

Some time ago, Donn Parker of SRI International, reported a survey which had been done by, I believe, the Institute of Internal Auditors, Inc. in the United States regarding the attitudes of people in the computer industry. The types of questions asked were such as: If someone else's program is on your computer, have you ever taken it? Do you feel there is any reason why you should not take it? There was a series of some 20 or 25 questions which, incidentally, can all be located for you. And basically, the shocking part was that most people in the computer field felt that they had a right to information in computers to which they had access; or felt they had a right to computers which were available to them in any way.

John Carroll of the University of Western Ontario also made a similar survey and found the same thing—that there seems to be lacking some degree of ethic. One thing I find very discouraging is that, in speaking to some heads of computer science departments in Canada, I find they seem to be saying, It is up to industry to give us the ethic; we do not know how to handle our students, and you should tell us. I think this is wrong. I think they are encouraging students to come into the business world without an ethic. They are forcing the businessmen to have to orientate and train these people. It is not a healthy climate.

You will recall when, a few years back, the problems of the University of Alberta led to prosecution. And prior to the prosecution, when the problems were first understood, there was the thought that they might even shut down the computer installation. Now, those are options which are just not available to us in business. It is not a question that you are going to shut down your computer.

[Translation]

Mais les responsables pensent que c'est un moyen moins coûteux de débrancher un système.

Dans l'industrie de l'informatique, on a longtemps eu des problèmes avec l'attitude des employés. Les employés spécialisés dans l'informatique se sont montré plus loyaux envers la technologie qu'envers leur employeur. Et maintenant, compte tenu de la conjoncture économique, l'ancienneté n'est pas nécessairement une garantie d'emploi, et la loyauté des gens envers la technologie est encore plus forte qu'auparavant. Les employés ont plus tendance à vouloir profiter de leur employeur.

Il y a également des problèmes au niveau de la sélection des employés. Compte tenu de la Loi sur les droits de la personne, nous n'avons pas toujours la possibilité de nous renseigner autant que nous le voudrions au sujet des gens que nous embauchons. C'est pourquoi nous pensons que l'utilisation du Code criminel serait un moyen dissuasif efficace.

Il y a quelque temps, Donn Parker, de la *SRI International*, a préparé un rapport sur une étude qui avait je pense été faite par l'*Institute of Internal Auditors, Inc.* aux États-Unis. Cette enquête portait sur l'attitude des gens au sein de l'industrie de l'informatique. On posait au répondant des questions du genre: Si votre ordinateur contient le programme de quelqu'un d'autre, l'avez-vous déjà pris? Selon vous, y a-t-il une raison pour laquelle vous ne devriez pas le prendre? Il y avait une série de 20 ou 25 questions, et si cela vous intéresse, je pourrais vous en procurer une copie. Il en est ressorti, ce qui est très choquant, que la plupart des gens interrogés pensent qu'ils ont droit aux renseignements que renferment les ordinateurs auxquels ils ont accès, et qu'ils ont droit aux ordinateurs qui sont d'une façon ou d'une autre à leur disposition.

John Carroll, de l'*University of Western Ontario*, a mené une enquête semblable et il en est arrivé à la même conclusion: L'éthique en a pris un coup. Ce que je trouve très décourageant c'est que certains chefs de département d'informatique au Canada avec qui j'ai eu l'occasion de discuter m'ont dit que c'est à l'industrie qu'il revient d'établir les normes de déontologie. Ils nous disent qu'ils ne savent pas quoi faire de leurs étudiants, et que c'est à nous de leur dire comment agir. Je ne suis pas d'accord. Je pense qu'ils encouragent les étudiants à se lancer sur le marché du travail démunis de tout sens de l'éthique. Ils obligent les hommes d'affaires à réorienter et à former ces gens. Tout cela ne crée pas un climat très sain.

Vous vous souviendrez que les problèmes qu'il y avait eus à l'*University of Alberta* il y a quelques années ont abouti à des poursuites en justice. Mais avant même l'instruction de l'affaire, lorsqu'on a pour la première fois compris la nature du problème, on avait même envisagé de fermer les installations informatiques. Ce genre de solution est impensable dans le milieu des affaires. Il n'est pas question pour un chef d'entreprise de débrancher son ordinateur.

The computer system has to keep running and so tampering in the business environment is a very serious offence.

Un ordinateur doit fonctionner en permanence, toute entrave constitue donc un délit grave.

[Texte]

There has been a lot of discussion whether or not computer abuse, if taken in its broadest sense, should be dealt with in the criminal code or whether it should not be handled under civil law. The businessman finds it very difficult to work within the civil law. He must prove his case; he must justify damages; it does not serve as a deterrent. As a matter of fact, there are many articles written and some thought that if you are going to commit a computer crime, it is not likely that you will be successfully prosecuted, and in this way computer abuse is encouraged.

I think this committee should know that there is a publication called *TAP*. Perhaps you know about it. I think it stands for "technology assistance program". It is a publication coming out of the States, originally designed for the telephone freaks and basically aimed against the telephone company, but it is a highly professional publication which explains to people how to violate computers. It also has some odds and sods about what to do about your guns and how to obtain them illegally and that sort of thing, but the impressive thing is that the quality of this publication is very high. These are not amateurs; these are professionals and they are broadcasting to their subscribers how to access computers illegally.

I think, when considering legislation, we are perhaps falling into the trap of tying legislation to technology. For example, much of our wording in the computer abuse, or would-be wording, relates to electronic or magnetic media and devices. If we had written this legislation or these words 20 years ago, we would have talked about electro-mechanical devices and, of course, it would have been obsolete by now. If we look to the future, we are going to be concerned with lasers and optical devices, fibre-optics—that sort of thing. I think it is very important that we tie legislation to actions and not to definitions. We spend a great deal of time worrying about the definition of data; we worry about the definition of computer and we worry about the definition of computer system; we really should be worrying about the action.

In my mind, in the business field any unauthorized use of a computer is offensive. It is not trivial. There are some people who would say that using the computer, though unauthorized, using time which no one else is using is trivial and therefore does no harm. The problem is that it is very difficult to determine at what point that so-called seemingly trivial action actually becomes meaningful and destructive and it may be that we never know. We know that there is great uncertainty about how much computer abuse exists today. We each have our own estimates. We know that seemingly the average computer crime amounts to hundreds of thousands of dollars. I think the popularly accepted figure these days is \$600,000 per crime whereas the white collar crime is probably in the range of \$1,900 . . . maybe the armed robbery crime is \$19,000. The point is that we do not know to what extent damages may be suffered by idle tampering and, therefore, it is important not to condone tampering in any way.

[Traduction]

La discussion bat son plein quant à savoir si oui ou non la «truandique», prise dans son sens le plus large, devrait relever du Code criminel ou du droit civil. Le droit civil pose beaucoup de problèmes à l'homme d'affaires. Il a la responsabilité de la preuve, la justification des dommages et l'effet dissuasif est inexistant. De nombreux articles ont été écrits, d'ailleurs, et s'agissant de crimes informatiques, il est fort peu vraisemblable que les poursuites aboutissent et la truandique est donc ainsi encouragée.

Il serait bon que vous connaissiez l'existence d'une publication intitulée *TAP*. Vous la connaissez peut-être. Je crois que *TAP* veut dire *technology assistance program*, «programme d'assistance technologique». Cette publication vient des États-Unis, et à l'origine elle était destinée aux pirates des téléphones et visait donc principalement les compagnies de téléphone, mais c'est une publication très professionnelle qui explique aux gens comment violer les ordinateurs. Elle donne également quelques explications sur le maniement des armes à feu et comment les obtenir illégalement, etc., mais ce qui impressionne c'est la très grande qualité de cette publication. Ce ne sont pas des amateurs, ce sont des professionnels et ils expliquent à leurs abonnés comment pénétrer les ordinateurs illégalement.

Pensant à une loi, nous faisons peut-être l'erreur de lier cette loi à la technologie. Par exemple, nombre des termes utilisés en matière de truandique, ou nombre des termes envisagés, se rapportent aux moyens d'information électroniques ou magnétiques et aux appareils. Si nous avions rédigé cette loi il y a 20 ans, nous aurions parlé d'appareils électro-mécaniques, et, bien entendu, cela serait aujourd'hui dépassé. Si c'est l'avenir qui nous intéresse, c'est de laser et d'appareils optiques, de fibres optiques, de ce genre de choses qu'il nous faudra parler. Il importe que nous liions la loi aux actes et non pas aux définitions. Nous consacrons beaucoup trop d'énergie à la définition de données, à la définition d'ordinateur et à la définition de système informatique alors que nous devrions en réalité la consacrer aux actes.

Pour moi, dans le domaine commercial toute utilisation non autorisée d'un ordinateur est choquante et non pas sans importance. D'aucuns prétendent qu'utiliser un ordinateur, même sans autorisation, que l'utiliser quand personne ne l'utilise est sans gravité et par conséquent inoffensif. Le problème est qu'il est très difficile de déterminer à partir de quel moment cet acte soi-disant sans gravité prend une importance réelle et devient destructeur et il se peut que nous ne le pourrions jamais. Nous savons qu'il est impossible aujourd'hui de mesurer avec certitude l'ampleur de la truandique. Nous avons tous nos propres chiffres. Nous savons qu'apparemment ces crimes informatiques correspondent à des centaines de milliers de dollars. Je crois que le chiffre généralement accepté aujourd'hui est de \$600,000 par crime alors que le crime de col blanc tourne probablement aux alentours de \$1,900 et que le crime à main armée tourne aux alentours de \$19,000. Nous ne connaissons pas l'ampleur des dommages provoqués par cette simple utilisation illicite et par conséquent, il importe de ne pas fermer les yeux.

[Text]

• 1555

I think an analogy I heard recently—and I think it was perhaps Donn Parker who made this analogy—was when someone accidentally knocks into someone in a corridor. If no harm is done and it is accidental, the people excuse each other and they go on. On the other hand, at some point, knocking into a person might injure that person, and it might be considered assault. It seems to me the important thing is that we have the ability to use the charge of assault, although we may decline to use it.

So I am suggesting, in the Criminal Code, any abuse of computers should be a criminal offence, but perhaps, depending on the circumstances, with the ability not to lay the charge.

We have a number of industry leaders, I guess, fathers of computers; and the computer industry is very complex. It has often been said, if the aircraft industry had grown as quickly as the computer industry has, we would have had a man on the moon in 1921.

I will quote one of our leaders, Adam Osborne. I was reading an article by him the other day. Osborne, who was considered the father of the micro-computer industry, points out there are just tremendous legal problems with computers, and they are so big he cannot hope to cope with them. Therefore, he is going to devote his energies to the better use of computers and not these legal matters.

Now, as a businessman, this tells me I cannot count on the industry to help me, that the problem is too big for them. Therefore, I have to turn to some legislative process to help give me the confidence and the necessary deterrence to protect my investment.

I worry very much about precipitous action, where legislation today may be tied down to today's terminology. I think we must focus on the actions or the activities. We must focus on unauthorized use, not on the consequences; and we must focus on the activities and not the objects of the action. In other words, we must not focus on the computers; we must focus on the protection of information. I think this is the key.

With that, I think that summarizes the essential message I want to make to this committee. I would welcome questions, and perhaps Mr. Rous would like to add something.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes, I was just going to ask if your colleague, Mr. Rous, would like to supplement what you have already stated.

Mr. Colin C. Rous (Cerberus Computer Security Inc.): Actually, Mr. Chairman, I was not going to supplement Jim's statement as much as to supplement his offer.

I was going to point out that Jim and I between us have been involved in computer security and privacy issues like this for

[Translation]

Dernièrement j'ai entendu Donn Parker, je crois, faire l'analogie avec deux personnes se bousculant accidentellement dans un couloir. S'il n'y a pas de dommage corporel et que c'est simplement accidentel, les deux personnes s'excusent mutuellement et poursuivent leur chemin. Par contre, si une des deux personnes blessent l'autre, on peut aller jusqu'à considérer cela comme une agression. Ce qui me semble important c'est que tout en y ayant recours rarement, cette possibilité d'accusation d'agression existe.

Dans le Code criminel, toute utilisation abusive d'ordinateur devrait être considérée comme une infraction criminelle, mais tout en conservant la possibilité de ne pas porter d'accusation selon les circonstances.

Nous avons toute une série de chefs de file, de pères de l'informatique et cette industrie est très complexe. On a souvent dit que si l'industrie aéronautique avait connu une croissance aussi rapide que celle de l'informatique, l'homme aurait posé le pied sur la lune en 1921.

Je vais citer un de nos chefs de file, Adam Osborne. Je lisais l'autre jour un de ses articles. Osborne, qui est considéré comme le père de la micro-informatique, dit que les problèmes juridiques en matière d'informatique sont tellement énormes qu'il n'a même pas l'espoir de pouvoir les régler. En conséquence, il a décidé de consacrer ses énergies à la meilleure utilisation des ordinateurs et non pas à ces questions juridiques.

En tant qu'homme d'affaires, cela me confirme que je ne peux compter sur l'industrie pour m'aider, que ce problème est trop vaste pour elle. En conséquence, je dois m'en remettre à la loi pour qu'elle rétablisse ma confiance et qu'elle me fournisse les moyens dissuasifs nécessaires à la protection de mon investissement.

Je crains énormément une action précipitée qui lierait la loi d'aujourd'hui à la terminologie d'aujourd'hui. Nous devons nous concentrer sur les actes ou les activités. Nous devons nous concentrer sur l'utilisation non autorisée, non pas sur les conséquences; nous devons nous concentrer sur les activités et non pas sur les objets de ces actes. En d'autres termes, nous ne devons pas nous concentrer sur les ordinateurs, nous devons nous concentrer sur la protection de l'information. Je crois que c'est la clé du problème.

Je crois que cela résume l'essentiel du message que je voulais vous transmettre. Je répondrai avec plaisir à vos questions et M. Rous voudra peut-être ajouter quelque chose.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'allais justement demander à votre collègue, monsieur Rous, s'il voulait ajouter quelque chose à ce que vous avez déjà dit.

M. Colin C. Rous (Cerberus Computer Security Inc.): En réalité, monsieur le président, je ne voulais pas tant ajouter quelque chose à la déclaration de Jim que m'associer à son offre.

Je voulais vous signaler qu'à nous deux, entre Jim et moi, nous représentons près de 25 ans d'expérience—additionnée,

[Texte]

about 25 years—jointly, obviously—and therefore, for that period of time, we have been very closely following legislation in other jurisdictions. We also hear an awful lot of the horror stories within industry that never make the press and are not even reported to the police, let alone to people like yourselves.

If I understand correctly, this subcommittee is just starting its task as a subcommittee; and therefore, the information you people have is the information you have so far as individuals. I was going to suggest we can serve you in two ways, and we are only here to provide you with information.

In the first place, we can give you a better than layman's point of view on what we suggest the business community would like to see in the way of legislation. Second—and I had not thought of this originally—for your own purposes, you might find it more instructive if we were to give you some background on the sorts of things that can happen and the consequences that can occur in the case of computer abuse.

• 1600

The thing I would like to add to this . . . and Jim has already referred to this—is that we do not know of any cases of computer abuse that could not have been prevented, given today's technology. These include the ones that have not been reported anywhere.

At first blush, that looks as though it is an argument against legislation. However, it is not. We believe extremely strongly that the legislation is required for the exact reasons that have already been referred to. Right now, this sort of activity is considered acceptable by society. We believe that the strongest way to tell people that this is not acceptable behaviour is to put legislation in place. Furthermore, we believe that this is an important step in educating the owners of computers to the responsibilities that they have to protect that data. As I said, they could have stopped it already; they have not, basically, because they are not aware. You people have an influence on that community that we will never have, that the news media will never have, and by saying this is right and this is wrong you people can go further than anybody else can to help solve the problem which is there. We believe that the legislation is critical.

As I said, we can, if you would like, fill you in on some of the things that have happened in the past. We can fill you in—with only freely available information, of course—on the ways that these things can happen: we would never consider putting on the public record any non-public ways of doing these things. It is entirely up to you what you would like us to do.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): Is this something that you would rather have another meeting in camera on?

Mr. Rous: Not necessarily. As I said, if we were to tell you things that were not already public knowledge we would first of all have to give you a six-month course in computer technology. So we would never get to a situation where we

[Traduction]

bien évidemment—en matière de sécurité informatique et de protection des biens privés et par conséquent, tout au long de ces années nous avons suivi de très près ce qui se faisait dans les autres juridictions sur le plan législatif. Nous sommes également au courant du nombre incroyable d'incidents qui ne sont jamais signalés à la presse ni même à la police et encore moins aux gens comme vous.

Si j'ai bien compris, votre sous-comité vient tout juste d'être constitué et par conséquent, pour toute information vous ne possédez que ce que vous connaissez personnellement. Je crois que nous pouvons vous servir de deux manières, et nous ne sommes ici que pour vous fournir des renseignements.

En premier lieu, nous pouvons vous indiquer, sur la base de notre expérience professionnelle, le genre de lois souhaitées par le monde des affaires. Deuxièmement—et je n'y avais pas pensé au départ—étant donné l'exercice dont vous êtes chargé, il se pourrait qu'il soit plus instructif que nous vous dressions un tableau général de la truandique et de ses conséquences.

J'aimerais ajouter—et Jim en a déjà parlé—que nous ne connaissons pas de cas de truandique qui n'aurait pu être prévenu, la technologie étant ce qu'elle est aujourd'hui. Cela inclut les cas qui n'ont jamais été signalés.

Au premier abord, cet argument peut sembler contraire à tout effort législatif. Il n'en est rien, cependant. Nous sommes convaincus qu'une loi est nécessaire pour les raisons précises qui ont déjà été indiquées. À l'heure actuelle, ce genre d'activité n'est pas condamné par la société. Nous croyons que le meilleur moyen de dire à la société que ce genre de conduite est condamnable est de légiférer. En outre, nous croyons que c'est important car cela ferait comprendre aux propriétaires d'ordinateurs les responsabilités qu'ils ont de protéger ces données. Comme je l'ai déjà dit, ils auraient déjà pu l'empêcher, ils ne l'ont pas fait, principalement, par ignorance. Vous exercez sur ces gens une influence que nous n'exercerons jamais, que les moyens d'information n'exerceront jamais, et en distinguant le bien du mal, vous ferez plus que quiconque pour nous aider à résoudre ce problème. Légiférer est donc crucial.

Comme je l'ai déjà dit, nous pouvons, si vous le souhaitez, vous rapporter certains des événements passés. Nous pouvons vous rapporter—à condition bien entendu, qu'il s'agisse de renseignements disponibles à tous—les différentes méthodes: il est hors de question que nous vous rapportions publiquement les méthodes qui n'ont jamais été publiées. Nous nous en remettons entièrement à vous.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Préférez-vous le faire à huis clos?

M. Rous: Pas forcément. Comme je l'ai déjà dit, si nous devons vous rapporter des choses inconnues du public, il faudrait tout d'abord que nous vous donnions un cours de six mois en technologie informatique. Nous ne vous donnerons

[Text]

were giving you information that could benefit somebody out there.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): We are in your hands. We are prepared to listen to anything that you can offer to us by way of additional information that is better than, as you say, the layman's view. Anything you can do to be helpful to this committee is more than welcome.

Mr. Rous: Are you aware of—I will pick a good example—the Dalton School case?

Mr. Beatty: Yes.

Mr. Rous: All of you? The University of Alberta case?

Mr. Beatty: Yes.

Mr. Rous: Okay. Are you aware of how the Dalton School case occurred, of technically what was done?

Mr. Beatty: What they had was a microcomputer at the Dalton School that a group of Grade 8 students used, using the phone system, and dialed an access into a number of data banks in Canada, some public, some private. I believe they probably used the micro to generate possible passwords until they finally found the key to the door and then subsequently were able to enter, I believe, two systems...

Mr. Rous: Absolutely correct.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): Maybe it would be helpful if you just put one or two or several of these illustrations on the record so the public would understand the kind of thing that we are really talking about at the moment.

Mr. Rous: Okay. This was a situation in which, as Mr. Beatty has said, the students, using a microcomputer, used public information—and this is the first key point: It is not hard to find out the telephone number of computers. That is as public information as people's phone numbers are. If you dial a computer, you will hear a high-pitched squeal instead of a voice saying hello. That tells you that you are now connected to a computer. You now basically send an automated signal to that computer saying: I am another computer and I would like to talk to you. The computer at that end says: Okay, who are you? You say: I am Joe Blow. That computer says: Okay, I know you are Joe Blow and you are allowed to be here; now tell me what you would like to do. Or else, as in the case of these kids, the computer says: I do not know any Joe Blow—click and hang up.

Now, what was done by these children was to take that computer and tell the other computer, first of all: I am Joe Blow. Did that work? No. I am Harry Schultz. Did that work? No. I am Sam Smith. Did that work? No. I am John Johnson. Bingo. The computer says: I know a John Johnson; talk to me. At that point they were on that computer just as an authorized employee of the company.

[Translation]

jamais de renseignements qui pourraient profiter à quelqu'un d'autre.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Nous vous faisons confiance. Nous sommes prêts à écouter tout ce que vous avez à nous offrir comme renseignements supplémentaires que votre expérience professionnelle vous a permis d'acquérir. Tout ce que vous pourrez nous communiquer pour nous aider sera le bienvenu.

M. Rous: Êtes-vous au courant—et je vais prendre un bon exemple—de l'affaire de l'école Dalton?

M. Beatty: Oui.

M. Rous: Tous? L'affaire de l'Université de l'Alberta?

M. Beatty: Oui.

M. Rous: Très bien. Savez-vous comment ils ont techniquement procédé?

M. Beatty: Un groupe d'étudiants de huitième année de l'école Dalton s'est servi du microordinateur en passant par le téléphone. Il a composé un numéro leur donnant accès à un certain nombre de banques de données du Canada, certaines publiques, certaines privées. Ils se sont fort vraisemblablement servis du microordinateur pour composer tous les mots de passe possibles et imaginables jusqu'à ce qu'ils finissent pas trouver la clef de la porte qui leur a permis de s'introduire, je crois, dans deux systèmes...

M. Rous: Absolument exact.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il serait peut-être utile que vous nous donniez plusieurs exemples de ce genre afin que le public comprenne exactement de quoi nous parlons.

M. Rous: Très bien. Comme M. Beatty l'a dit, les étudiants, utilisant un microordinateur, se sont servi de renseignements publics—et c'est le premier point important: il n'est pas difficile de trouver le numéro téléphonique d'un ordinateur. Ils sont répertoriés tout comme les numéros téléphoniques des particuliers. Si vous appelez un ordinateur, au lieu d'une voix, c'est un son très aigu qui vous répond. Cela vous indique que vous êtes maintenant lié à un ordinateur. Vous envoyez alors, en gros, un signal automatisé à cet ordinateur lui disant: je suis un autre ordinateur et j'aimerais vous parler. L'ordinateur répond: d'accord, qui êtes-vous? Vous répondez: je suis Joe Blow. L'ordinateur poursuit alors en disant: je sais que vous êtes Joe Blow et que vous avez l'autorisation nécessaire; dites-moi maintenant ce que vous voulez faire. Ou bien, dans le cas de ces enfants, l'ordinateur répond: je ne connais pas de Joe Blow et il raccroche.

Ce que ces enfants ont fait c'est qu'ils ont tout d'abord dit à l'autre ordinateur: je suis Joe Blow. Est-ce que cela a marché? Non. Je suis Harry Schultz. Est-ce que cela a marché? Non. Je suis Sam Smith. Est-ce que cela a marché? Non. Je suis John Johnson. Bingo. L'ordinateur a répondu: je connais un John Johnson: parlez-moi. À partir de ce moment, ils ont eu accès à cet ordinateur tout comme n'importe quel employé autorisé de la compagnie.

[Texte]

How do you stop that? Well, in the first place, the computer that they were tapping into thought they were an authorized user. They could have been stopped technically in a variety of ways. The companies that could have stopped them did not stop them. But the key thing—and here is the part we were referring to earlier about the educational community, and I realize this is for the public record—there is a strong suspicion among people like us, although we cannot prove this, that those 13-year-old boys had assistance from far more senior people, perhaps on the faculty. They subsequently did a lot more things like that, that we heard reported, that are not on public record.

• 1605

As long as you have people out there who are accepting the challenge of breaking this sort of thing, we are in big trouble. Because the companies they broke into said, aha, this has happened to us, so now what we will do is, if somebody tries three times and they do not succeed, we will say that is somebody trying to break into us, so we will not let them dial up again. There is a technical solution. As soon as I put that technical solution in place, these kids start researching deeper and deeper, saying, okay, how do I beat that one? So they beat it. I say, all right, now we know what they did. How do I stop that? I put another measure in place. They say aha, they stopped me doing it this way. It is a war of wits that is going on constantly. It is the same sort of war of wits that goes on among people trying to forge public transit monthly passes or anything else, except that the consequences are infinitely greater. We do not know of any way today in which you can produce a completely secure computer system. It cannot be done. Describe to me any computer system and I can, both theoretically and practically, figure out ways to break it. One of the finest examples of this: Several years ago the United States government in concert with several research organizations set out specifically to design a secure computer. It was called Project Mac. The end result of the project was a commercial computer which is available out on the market right now. In the course of developing it, the government specifically invited all of the experts they could find to try to tap into this computer. Keep breaking it; as soon as you break it, we will find out what you did and we will build in safeguards against that. Keep breaking it; try it again, try it again, try it again. Finally, one day the project manager said, all right, now we have it. We have blocked off every loophole these people would ever be able to find. So they called their big project meeting. It took place in a large auditorium down in the States and there were about 100 people in the audience. The project leader stood up at the front and said: Gentlemen, we have now done it. Project Mac is secure. Two military gentlemen in uniform looked at each other, smiled, got up and left the room, came back 10 minutes later, walked up to the podium and handed the chairman a list of every password for every authorized user of this new, totally secure computer system. The point is, we cannot prevent it.

[Traduction]

Comment l'empêcher? En premier lieu, l'ordinateur sur lequel ils s'étaient branchés pensait qu'il s'agissait d'un usager autorisé. Ils auraient pu être arrêtés techniquement de diverses manières. Les compagnies qui auraient pu les arrêter ne l'ont pas fait. Mais l'important—et c'est ce dont nous parlions un peu plus tôt au sujet du monde de l'éducation; et je sais que nous sommes en séance publique—c'est que les gens comme nous soupçonnent fortement, bien que nous ne puissions le prouver, que ces garçons de 13 ans ont bénéficié de l'aide de personnes beaucoup plus âgées, peut-être de membres du personnel de la faculté. Par la suite, ils ont fait bien d'autres choses qui n'ont pas été rapportées publiquement mais dont nous avons entendu parler.

Tant qu'il y aura des gens prêts à se livrer à ce genre d'infraction, nous aurons de gros problèmes. Les compagnies victimes de ces intrusions, apprenant ce qu'il leur était arrivé, ont décidé que si quelqu'un essayait trois fois d'entrer en communication sans réussite, ce sera la preuve que quelqu'un essaie d'entrer illicitement en communication et leur ordinateur ne répondra plus à la sollicitation. C'est une solution technique. Dès que je mets en place cette solution technique, ces enfants se remettent à chercher le moyen de contourner cet obstacle. Ils y arrivent. Je me dis: nous savons maintenant comment ils ont procédé. Comment les en empêcher? Je prends une autre disposition. Ils la contournent de nouveau. C'est une bataille de cerveau qui se poursuit sans cesse. C'est le même genre de guerre d'invention que celle à laquelle se livrent ceux qui fabriquent de fausses cartes mensuelles de transport public, par exemple, si ce n'est que les conséquences sont infiniment plus grandes. Nous ignorons aujourd'hui comment construire un système informatique à l'abri de toutes intrusions. Ce n'est pas possible. Décrivez-moi un système informatique et je peux, théoriquement et pratiquement, trouver le moyen d'y avoir accès. Je vais vous citer un des plus beaux exemples. Il y a plusieurs années, le gouvernement des États-Unis de concert avec plusieurs organismes de recherche s'est appliqué à concevoir un ordinateur à l'abri de toutes intrusions. C'était le projet Mac. Le résultat de ce projet a été un ordinateur commercial qui est actuellement en vente sur le marché. Pendant la mise au point, le gouvernement a invité tous les spécialistes à trouver tous les moyens possibles d'accéder à cet ordinateur. Essayez tous les moyens, et chaque fois que vous réussirez, nous trouverons ce que vous avez fait et nous ajouterons les systèmes de protection en conséquence. Essayez, essayez, essayez. Finalement, un jour le directeur du Projet a dit: très bien, nous avons maintenant trouvé. Nous avons bloqué toutes les entrées illicites que ces gens avaient pu trouver. Ils ont donc convoqué leur grande assemblée de fins de projet. Elle a eu lieu dans un grand auditorium aux États-Unis et environ 100 personnes étaient présentes. Le directeur de projet a pris la parole et a dit: Messieurs, nous avons réussi. Le projet Mac est à l'abri de toutes intrusions. Deux militaires en uniforme se sont regardés, ont souri, se sont levés et ont quitté la salle, sont revenus 10 minutes plus tard, ont marché jusqu'au podium et ont donné au président la liste de tous les mots de passe pour chacun des usagers autorisés de ce nouveau

[Text]

Not too long ago we had a client who suffered a quarter of a million dollar fraud. The way this one happened was, they had a receiving clerk on the receiving dock who had a terminal. This is more and more common in companies now. The average company starting to computerize has anywhere from a dozen to several hundred video screen terminals out there. In this particular situation, this fellow's job, when a shipment arrived at the loading dock, was to go to the terminal and key in the information: Yes, we received a shipment of such and such. He rapidly discovered there was a little loophole there. Now, it is very hard to think of every loophole. What he figured out is, because he was working late at night by himself, he could sit down and he could enter into his terminal a purchase order. Now, the computer did not know whether he was the purchasing manager or Joe Blow from the street. So he would enter a purchase order for clay pipe. He would wait a week or two, the average length of time it would take for a shipment to be received, and then he would sit down at his terminal and he would say to the computer, this clay pipe has now been received. The computer would say, we had a purchase order, we have received the goods; send out the cheque. What the computer could not know, of course, is the company they were sending the cheque to was a dummy company set up by him and an accomplice of his. They got away with a quarter of a million dollars, and the only way they got caught was because this particular company did not deal in clay pipe. When they finally got a little greedy and ordered \$80,000 worth of it at once, somebody said, why are we ordering \$80,000 worth of clay pipe? That is when they discovered it. Again, an extremely difficult situation for us to stop.

Probably one of the classic cases, which again illustrates this sort of ease, was done in New York—and this is a fairly well known case from quite a few years ago. There was a raid by the New York City police on a bookmaker, and they discovered a fellow who was betting an average of \$30,000 a week, sometimes winning, sometimes losing. But they figured anybody betting \$30,000 a week was worth looking at, so they investigated and discovered he was a bank teller earning \$13,000 a year. That got them a little curious.

Mr. Beatty: Maybe he saved a lot.

Mr. Rous: That was the first question and they rapidly realized that was probably not the case. What he had done, and this again is very tricky if you stop and think about it, he would pull funds out of people's accounts into his own account. He knew when the auditors were coming, their own bank's auditors, so whenever a particular group of accounts was going to be audited, he would throw the funds back into those accounts for the duration of the audit and then pull them back out again. Okay. So now he has money shuffling back and

[Translation]

système informatique à l'épreuve de toutes intrusions. C'est une impossibilité.

Il n'y a pas longtemps, nous avons eu un client ayant souffert d'une fraude d'un quart de million de dollars. Cette compagnie avait un commis responsable des réceptions à l'entrepôt qui possédait un terminal. C'est de plus en plus courant dans les compagnies. Les compagnies moyennes qui commencent à s'informatiser peuvent avoir d'une douzaine à plusieurs centaines de terminaux à écrans. Dans ce cas particulier, le travail de cet employé, lorsqu'une expédition arrivait à l'entrepôt de chargement, était d'introduire dans le terminal le renseignement suivant: oui, nous avons reçu un chargement de tel ou tel produit. Il a rapidement découvert qu'il y avait une petite faille. Il est très difficile de penser à tout. Étant donné qu'il travaillait tard le soir tout seul, il a compris qu'il pouvait faire entrer dans son terminal une commande d'achat. L'ordinateur ne savait pas si c'était le directeur des achats ou Joe Blow qui faisait entrer cette donnée. Il faisait donc entrer une commande d'achat de tuyaux en argile. Il attendait une semaine ou deux, le temps moyen pour qu'une commande arrive, puis par l'intermédiaire de son terminal, il disait à l'ordinateur le tuyau d'argile est maintenant arrivé. L'ordinateur répondait: nous avons reçu une commande d'achat, nous avons reçu la marchandise; envoyez le chèque. Ce que l'ordinateur ne pouvait savoir, bien entendu, c'est que la compagnie à laquelle il envoyait le chèque était une compagnie fantôme créée par l'employé et par un complice. Ils ont réussi à soutirer un quart de million de dollars, et s'ils se sont faits prendre c'est parce que cette compagnie ne vendait pas de tuyau en argile. Lorsqu'ils sont devenus un peu trop gourmands et qu'ils en ont commandé pour \$80,000 d'un seul coup, quelqu'un s'est demandé, pourquoi commandons-nous pour \$80,000 de tuyau en argile? C'est ainsi qu'ils se sont faits prendre. Il nous est très difficile de prévenir ce genre de malversation.

Un des cas les plus célèbres probablement et qui est une illustration parfaite s'est passé à New York. Cela remonte à un certain nombre d'années et cette affaire est assez bien connue. La police de New York a fait une descente chez un *bookmaker* et elle a découvert qu'un type pariait une moyenne de \$30,000 par semaine, gagnant parfois, perdant parfois. Elle s'est dit que quelqu'un pariant \$30,000 par semaine valait la peine d'être retrouvé, elle a donc enquêté et découvert que c'était un employé de banque gagnant \$13,000 par an. Leur curiosité a été éveillée.

M. Beatty: Il avait peut-être beaucoup d'économies.

M. Rous: C'est la première question que la police s'est posée mais elle a rapidement compris que ce n'était probablement pas le cas. Ce qu'il faisait, et encore une fois, c'est très ingénieux si vous y réfléchissez, c'était transférer les fonds des comptes de certains clients sur son propre compte. Il savait quand les vérificateurs venaient, les vérificateurs de sa propre banque, si bien que chaque fois qu'un groupe particulier de comptes devait être vérifié, il reversait les fonds dans ces comptes pendant la durée de la vérification puis les transférait

[Texte]

forth through that company like mad, but he was in a sensitive enough position to know when the audits were coming. He could have gotten away with that for years and years and years except for the fluke of a raid on a bookmaker's joint, totally unrelated to what he was doing. Again, how would we have stopped that? It is very, very difficult for us to find every one of those loopholes, and as soon as we find one, they are going to find another one. This is why even though—and I am the first to say this; I say this to all of our clients: Listen, gentlemen, there is nothing you could not prevent today. Even though that is theoretically true, there is nobody out there in the business community that is omniscient. Nobody could find it all.

We had another situation in which a company was being consistently underbid by pennies on every contract. We never solved that one. We do not even know whether the information was being stolen from the computer. We put a bunch of security measures in place and it got stopped. We will never know how it happened. Okay, another indication. We will never know. We do not know what happened there. Companies have become so dependent upon the computers—it is estimated that within the next five or six years, there will be two terminals for every three employees in the average office. That is not my estimate; that is an estimate that has been done by several highly reputed forecasting firms. Two terminals for every employee. Now when you figure that every one of those terminals is a gateway into that computer system and you figure that that computer system is being used for more and more and more of the business, you realize that we have a major problem.

We are a very small company ourselves and yet our own planning is computerized, our future plans as well as our accounting results. If we are doing that, think about what the Imperial Oils and the General Motors and the IBMs are doing. Everything is there now. I have all of the personnel evaluations of my senior employees; I have my career plans; recorded in the computer is where I expect to open plants. Think of the value of that sort of information for somebody who is thinking of speculating in real estate. The damage that can be done has become incalculable and the complexity of the systems has become such that we can no longer protect them and on top of that, it is very much the same sort of situation as bank robberies back in the 1930s. The perpetrators of these offences are folk heroes. Now what can we do when somebody gets away with it or gets caught even but the public consider him a hero. One of the classic examples of this is one of the early discovered computer crimes, a young highschool student who stole about \$800,000 from Pacific Telephone and Telegraph. He was eventually captured, convicted and his sentence was 60 days; of that he served 40. When he left prison, he had a brief career as a computer security consultant. Now that lasted less than a year. Finally, his clients took a look and said, wait a minute, why are we using a crook. But the point is \$800,000 for 40 days in jail? Sounds like a pretty good deal to me and that was in a jurisdiction that treated things much more strongly, much more seriously, than many other jurisdictions do.

[Traduction]

de nouveau. Il faisait faire une navette incroyable à ces fonds, mais il occupait un poste lui permettant de connaître les dates de vérification. Il aurait pu continuer pendant des années si ce n'avait été de cette descente fortuite n'ayant rien à voir avec ce qu'il faisait. Comment aurions-nous pu l'empêcher? Il nous est extrêmement difficile de détecter chacune de ces failles, et dès que nous les trouvons, ils en trouvent d'autres. C'est pourquoi même si, et je suis le premier à le dire, je le dis à tous nos clients: Messieurs, il n'y a rien que vous ne puissiez empêcher aujourd'hui. Même si théoriquement c'est vrai, personne n'est omniscient, personne ne peut tout trouver.

Nous avons eu également l'exemple d'une compagnie qui se faisait constamment souffler ses contrats pour une question de cent. Nous n'avons jamais trouvé la solution. Nous ne savons même pas si les renseignements étaient volés dans l'ordinateur. Nous avons mis en place une série de mesures de sécurité et cela a cessé. Nous ne saurons jamais ce qui s'est passé. C'est un autre point. Nous ne saurons jamais. Nous ne savons pas ce qui s'est passé. Les compagnies sont devenues si dépendantes des ordinateurs, il a été calculé que d'ici cinq ou six ans, il y aura deux terminaux pour trois employés dans pratiquement tous les bureaux. Ce calcul n'est pas de moi, c'est un calcul qui a été fait par plusieurs firmes de prévisions de très grande réputation. Deux terminaux pour trois employés. Quand on sait que chacun de ces terminaux correspond à une porte d'entrée dans le système informatique et quand on sait que ce système informatiques sont de plus en plus utilisés dans les transactions, on comprend l'importance du problème.

Nous ne sommes nous-mêmes qu'une très petite compagnie et pourtant notre propre planification est informatisée, nos programmes et notre comptabilité le sont également. Si nous le faisons, pensez à ce que font *Imperial Oils*, *General Motors* et *IBM*. Tout est dans la machine. J'ai toutes les évaluations personnelles de mes cadres; j'ai mes plans de carrière; dans l'ordinateur se trouvent les endroits où j'ai l'intention d'ouvrir des usines. Pensez à la valeur de ce genre de renseignement pour quelqu'un qui s'intéresse à la spéculation foncière. Les dommages potentiels sont devenus incalculables et la complexité des systèmes est devenue telle que nous ne pouvons plus les protéger et de plus, nous nous retrouvons dans le même genre de situation qu'au moment des vols de banque dans les années 30. Les coupables de ces délits sont considérés comme des héros populaires. Que pouvons-nous faire quand les criminels ne se font pas prendre ou s'ils se font prendre et que le public les considère comme des héros. Un des exemples classiques est un des premiers crimes informatiques ayant été découvert, celui perpétré par un jeune étudiant qui avait volé environ \$800,000 à *Pacific Telephone and Telegraph*. Il a finalement été capturé et condamné à 60 jours, dont il n'a servi que 40. Lorsqu'il est sorti de prison, il a fait une brève carrière comme consultant en sécurité informatique. Cela n'a duré qu'un peu moins d'un an. Finalement, ses clients se sont dit, un instant, pourquoi consultons-nous un escroc. Il reste: \$800,000 pour 40 jours de prison? Cela me semble une excellente affaire et c'était une juridiction beaucoup plus sévère et beaucoup plus sérieuse que nombre d'autres.

[Text]

Mr. Beatty: May I perhaps interrupt to ask one or two questions. I think it has been a very useful exposition for us of your perspective as security consultants and also of the seriousness with which business views this. I was particularly struck by the reference that you made to the difficulties in using the civil law, from a business' point of view, to deal with a problem like this.

Could I first of all ask you whether you feel it is a fair analogy that can be made, perhaps to simplify things, between computer crime and bank robbery; that there is no physical system for storing money which is 100% secure. Any system can be breached. It is simply a matter of the complexity and the cost that is involved in breaching it. You can always make it more secure than it was but it can never be 100% secure. Is that correct?

• 1615

Mr. Rous: Yes.

Mr. Beatty: So, it would be analogous in that regard. What we are talking about is that physical security and legal protection must complement each other; that passing a law does not obviate the need for you fellows to put in proper security on computers, but it assists you in ensuring that there is some protection for the data.

Mr. Rous: One hundred per cent. Neither one is a solution by itself. The two together give us a better possibility, a better chance than we have today.

Mr. Beatty: Could you just give us some sort of perspective on how serious the potential is? When officials from the Justice Department met with us last week, they tabled for us a copy of an article from *CA Magazine* in January 1981, an article by Peter Watkins who is with Peat, Marwick and Partners. The headline was "Computer Crime: Separating the Myth from the Reality", and it says underneath: "It's the crime figures that are suspect." In essence, Mr. Watkins attempts to debunk the Donn Parker or the John Carroll suggestions that we are just seeing the tip of the iceberg. From your experience, how serious is it? The OPP have said that they have undertaken a survey which indicates that even privately the incidence of computer crime is very low.

Mr. Rous: I was going to say both the RCMP and the FBI refuse to even collect—well, no, I cannot say that—refuse to divulge statistics because the statistics are so meaningless. The OPP study was an extremely interesting one, but they will be the very first to tell you that there is no statistical validity in what they did. It was an illustrative study that was done and it can be treated almost anecdotally. You cannot prove that it was statistically valid, in any way, shape or form.

The figure that gets tossed around is 85% of computer crimes go unreported. Now, that is really instructive. The fellow who first promulgated that figure did it several years ago—quite a few years ago—and he meant it as an ironic statement, because how can you say that 85% go unreported? If any are going unreported, how can you say how many are going unreported? Right. Unfortunately, there were some members of the press in the audience when he was speaking

[Translation]

M. Beatty: Pourrais-je vous interrompre pour vous poser une ou deux questions? Cet exposé de votre point de vue de consultant en sécurité ainsi que la gravité avec laquelle le monde des affaires considère le problème sont très intéressants. Ce qui m'a tout particulièrement frappé c'est que vous ayez parlé des difficultés de recours au droit civil, du point de vue des hommes d'affaires, pour régler ce problème.

Pourrais-je tout d'abord vous demander si selon vous, il est juste de faire une analogie, peut-être pour simplifier les choses, entre les crimes informatiques et les vols de banque; il n'y a pas de système physique permettant d'entreposer l'argent avec une sécurité totale? Il n'y a pas de système qui soit inviolable, la seule variante est la complexité et le coût qu'il faut encourir pour procéder à l'effraction. Vous pouvez toujours améliorer la sécurité mais elle ne sera jamais parfaite. Est-ce exact?

M. Rous: Oui.

M. Beatty: Il s'agit donc de faire en sorte que la sécurité physique et la protection juridique se complètent l'une et l'autre; l'adoption d'une loi n'écarte pas la nécessité dans laquelle vous êtes de protéger vos ordinateurs mais assurerait au moins une certaine protection de vos données.

M. Rous: Absolument. Aucune des deux méthodes ne suffit à résoudre le problème, par contre les deux ensemble créent des conditions plus favorables qu'aujourd'hui.

M. Beatty: Pourriez-vous nous donner une idée de la gravité du problème? Lorsque nous avons rencontré les fonctionnaires du ministère de la Justice la semaine dernière, ils nous ont remis une copie d'un article du *CA Magazine* de janvier 1981 écrit par Peter Watkins du Cabinet Peat, Marwick et Partners. Il était intitulé «Criminalité informatique»: Faire la part du mythe et de la réalité et disait en substance que ce sont les statistiques sur cette criminalité qui sont suspectes. Il s'oppose à l'idée que Donn Parker et de John Carroll voulant que nous ne connaissions que la pointe de l'iceberg. Selon vous, quelle est la gravité du problème? La police provinciale de l'Ontario a entrepris une étude qui montre que l'incidence de la criminalité informatique est très faible même dans le secteur privé.

M. Rous: J'allais dire que la GRC aussi bien que le FBI refusent de réunir—non je ne puis pas dire cela—refusent de divulguer des statistiques car elles sont si peu fiables. L'étude de l'OPP est extrêmement intéressante mais ils seront les premiers à reconnaître l'invalidité des méthodes statistiques qu'ils ont suivies. C'est une étude de cas en quelque sorte qui n'a guère de valeur qu'anecdotique. Il est impossible de prouver qu'elle ait une valeur statistique quelconque.

On cite généralement le chiffre de 85 p.100 des infractions qui ne sont jamais découvertes. Cela est très instructif car ce chiffre a été lancé il y a plusieurs années plus ou moins à titre de canular car comment peut-on affirmer que 85 p.100 des délits ne sont jamais détectés? S'ils ne sont pas détectés, comment peut-on les compter? Evidemment. Malheureusement il y avait des journalistes dans l'audience qui n'ont rien compris à la plaisanterie mais qui ont répandu ce chiffre

[Texte]

who totally missed the irony of his statement, and within hours it was being broadcast as an authoritative statement on what happens with computer crime. Therefore, you see some horrendous projections where people—Donn Parker, for example, does a very good job of collecting the ones that are reported. So somebody takes and collects Donn Parker's figures for the year 1978 and says, that was 15%; therefore, in 1978 losses were that divided by 0.15. We do not know. We honestly, truly do not know. However, at another time, if you would like, we could sit down and we could prove how easy it would be for us to bankrupt virtually any company you could think of, and I mean bankrupt, and I mean quickly. The potential is so great. The incidents that have occurred, have occurred so easily that regardless of what the true statistics are we believe the situation is critical.

The one thing that has saved us so far is that the vast majority of computer abuses that have been carried out have been done by people such as students who are doing it for intellectual challenge. If the people who had carried those out had been out to make a buck, they would have made a buck.

Mr. Beatty: You have put your finger on what was going to be my next question, I guess, and that is the potential for very serious damage to be done to business by this. To what extent are businesses dependent on—if, for example, the hacker were to get into a corporate computer, could you find that a system crash would be enough in itself possibly to bankrupt a corporation?

Mr. Rous: Definitely—100%. Now that depends, of course, upon the type of business. Some of the best examples are hotel and airline reservation systems. Ottawa is a nice example. Ottawa is full of hotels that are parts of chains. If I am in Toronto and I want to come up to Ottawa, and I phone the Sheraton for a reservation in Ottawa and the Sheraton's computer system is down, I am not going to wait and say, please call me back in three hours when your computer is back up again. I am going to phone Hilton and make a reservation. If their computer system stays down for a number of days, they will start hitting a situation where they are not getting reservations to any of their hotels anywhere.

• 1620

We all know that is the kind of business in which people develop loyalties. I come to a hotel in Ottawa; it treats me well and I come back to that one again. It would not take long for a company like that, or an airline or a bank with on-line banking facilities, to be driven out of business completely by purely and simply lack of availability, crashing the system. If I can crash it and make it stay down, I could bankrupt that company.

Mr. Beatty: Do we have any inventory as to what extent data bases are on line and it is possible to get dial-in access to them in Canada? I gather your concern goes well beyond data bases with dial-in access; you are also dealing, for example, with employees of companies who would be operating *in situ*, if you like. But do you have any inventory of how many

[Traduction]

partout comme venant de source sûre. C'est ainsi qu'on voit des estimations aberrantes... Par exemple, Donn Parker, fait une très bonne compilation des infractions qui sont découvertes. Quelqu'un prend donc les chiffres de Donn Parker pour l'année 1978 et considère qu'ils représentent 15 p.100 de la criminalité totale. Cela ne signifie rien, car nous ne sommes dans la plus complète ignorance. Par contre, nous pouvons très bien réfléchir à un problème donné et montrer combien il serait facile de mettre en faillite complète n'importe quelle entreprise et cela très rapidement. Le potentiel est énorme. Les détournements qui se sont produits étaient d'une telle facilité que nous jugeons la situation très critique, quelle que soit leur fréquence.

Ce qui nous a sauvés jusqu'à présent, c'est que la grande majorité des détournements ont été le fait de gens comme des étudiants qui voyaient là un défi intellectuel. S'ils l'avaient fait par appât du gain, ils auraient pu se remplir les poches.

M. Beatty: Vous avez mis là le doigt sur la question suivante qui est le risque qu'encourent les établissements commerciaux. Dans quelle mesure leur fonctionnement est-il à la merci—si par exemple un plaisantin trouve accès à l'ordinateur d'une société et en efface le mémoire, cela ne suffirait-il pas à la mettre en faillite?

M. Rous: Certainement, à 100 p. 100. Tout dépend évidemment du genre d'entreprise. Les plus vulnérables sont les systèmes de réservation des hôtels et des compagnies aériennes. Ottawa en est un très bon exemple car la ville est pleine d'hôtels qui font partie de chaînes. Si, habitant à Toronto, je veux séjourner à Ottawa, je téléphone au Sheraton pour avoir une réservation et si l'ordinateur de la chaîne est en panne, je ne vais pas attendre trois heures pour avoir confirmation de ma réservation. Je vais téléphoner plutôt au Hilton et réserver chez eux. si leur système informatique est hors service pendant plusieurs jours, ils n'obtiendront plus de réservation dans aucun de leurs hôtels.

Nous savons tous que c'est un secteur où les gens prennent des habitudes. Je séjourne dans un hôtel à Ottawa, je trouve que l'on m'y traite bien et j'y reviendrai la prochaine fois. Il ne faudrait pas longtemps pour qu'une chaîne d'hôtels, ou une compagnie aérienne ou une banque avec terminaux en ligne disparaisse simplement parce que les clients n'y auraient plus accès, par effondrement du système informatique. Si je peux le mettre en panne et l'y maintenir, je peux mettre l'entreprise en faillite.

M. Beatty: Saurons-nous dans quelle mesure les banques de données sont en ligne et accessibles par téléphone? J'imagine que votre inquiétude ne se limite pas aux banques de données accessibles de l'extérieur mais embrasse également les actes de malveillance que peuvent commettre des employés sur place. Connaît-on le nombre des établissements commerciaux dont le système informatique est accessible par téléphone au Canada?

[Text]

companies would have computers with dial-in access in Canada?

Mr. Rous: No, but we could locate those figures quite quickly. In fact, the quickest source of those would be CN/CP and Bell Canada. If you added up those two, then all you have are the private networks. There is a number of private networks on top of that, but a summary of the dial-up ports those two have would be a pretty quick estimate of the inventory.

Mr. Beatty: Let me refer back again to the Dalton school incident. I believe at least two of the computer systems the students tried to access were federal government computers. In neither case were they successful in breaking in. In your judgment, are files that are kept in federal data banks with dial-in access secure?

Mr. Rous: That is a question we would rather not answer. We have not done too many official contracts with the federal government, and we try to keep our clients' specific situations confidential, anyway. So we cannot answer that from our personal knowledge. We could give you a guess; but because we are speaking for the record, I would rather not do that.

Mr. Beatty: Certainly.

Mr. Finch: Could I come back on some of those questions, maybe on this last one first? Certainly, in business, we find the records are not safe, often because the businessman just has other higher priorities.

I would like to go back, Mr. Beatty, into some of the previous points Colin has been responding to. You asked about a system crash. You will recall, back in the 1950s, I think it was Eaton's that lost millions of dollars simply because they lost their records.

Now, that is a long time ago and it is old history; but with the cost of computers coming down, the number of computers in use is increasing tremendously. These systems and the users of these systems are just learning how to back up their systems. Eaton's had difficulties because they were not able to recover; they were not able to back up those files.

These are not just users of micro-computers or personal computers. These are businesses probably in the \$2 million to \$10 million range annually, which have reasonably sophisticated systems; and yet, they are just learning now how to back them up. It is in an infancy stage.

The characteristic of all the new systems today is that they are interactive. That means the data is entered through terminals. Now, it is not just the fact that you may be able to dial into that system. The question is: Can you get access to a terminal that is on the system? I think this opens up the opportunity much more. I think all of us have walked by a terminal in an office or in a building somewhere that we had no right, obviously, to access or to use; but we could have.

We have a much more computer-literate public today than ever. Today, with the proliferation of the personal computers,

[Translation]

M. Rous: Non, mais on pourrait trouver ce chiffre assez rapidement. La source la plus rapide serait le CN/CP et Bell Canada. Si vous faites la somme des deux, il ne reste plus alors que les réseaux privés. Il en existe un certain nombre mais la majorité des postes d'accès téléphonique appartiennent à ces deux-là.

M. Beatty: Revenons à l'incident de l'école Dalton. Je crois savoir que deux des systèmes informatiques auxquels les étudiants ont essayé de trouver accès étaient des ordinateurs du gouvernement fédéral. Ils n'y sont parvenus dans aucun des deux cas. Existe-t-il, à votre avis, des banques de données fédérales accessibles à distance?

M. Rous: Je préfère ne pas répondre. Nous n'avons pas effectué beaucoup de travaux pour le gouvernement fédéral et nous préférons rester discrets sur les situations spécifiques de nos clients. Nous ne pouvons pas répondre sur la base de ce que nous savons de première main. Nous pourrions vous donner une conjecture, mais vu le caractère officiel de cette audience, je m'en abstiendrai.

M. Beatty: Bien.

M. Finch: J'aimerais revenir sur certaines de ces questions, et notamment sur la dernière. Dans le secteur privé, la sécurité des archives n'est pas toujours assurée, principalement parce que l'entreprise a d'autres priorités.

Monsieur Beatty, j'aimerais revenir sur certaines des questions auxquelles Colin a répondu. Vous avez mentionné l'effondrement des systèmes. Dans les années 50, vous vous souviendrez que Eaton a perdu des millions de dollars simplement à cause de la destruction de ses archives.

Cela est maintenant devenu de l'histoire ancienne mais la baisse de prix entraîne une multiplication foudroyante du nombre des ordinateurs. Leurs acquéreurs commencent seulement maintenant à apprendre à s'en servir, à se constituer des données de secours. Eaton s'est trouvée en difficulté parce qu'il n'y avait pas d'archives de rechange, une fois qu'elles étaient perdues, c'était fini.

Nous ne parlons pas là des micro-ordinateurs ou d'ordinateurs individuels. Nous parlons d'entreprises qui ont un chiffre d'affaires annuel de l'ordre de 2 à 10 millions de dollars et qui possèdent des systèmes relativement sophistiqués et qui commencent seulement maintenant à se doter de systèmes de secours. Elles en sont encore au tout début.

Tous les nouveaux systèmes aujourd'hui se caractérisent par le fait qu'ils sont interactifs, c'est-à-dire que l'accès se fait par des terminaux. Le problème n'est pas seulement qu'on puisse y accéder par branchement téléphonique, les terminaux installés dans les entreprises sont eux-mêmes vulnérables. Je pense qu'il nous est arrivé à tous de nous trouver devant un terminal dans un bureau quelque part, que nous aurions pu utiliser sans y être autorisé.

Le public est aujourd'hui beaucoup mieux renseigné qu'avant. Avec la prolifération des ordinateurs individuels,

[Texte]

almost all the young people know what to do when they step up to a computer terminal. The mystique of the computer is disappearing. Some people have indicated great concern that we are breeding a generation of computer thieves. I do not like to look at it in that sense. I like to think there will always be an element of society that turns to abuse; but by more of us understanding the machines we are dealing with, in fact, we will be better prepared to prevent it.

• 1625

The number of systems that could be accessed is tremendous. Recently I visited, in one evening, four computer utilities and I was successful in three of them in walking right into the machine room through so-called security guards and barriers, and so forth, without using any physical violence. I must admit that in one case I signed in a fictitious name at the door and went to a different floor from the one I was supposed to. So, from our professional point of view, we had a great challenge in educating these people not to expose themselves to computer abuse. Certainly the ability to access these systems . . . I would issue to you an unofficial challenge that Rous here, my partner, can crack any system in the country and I think probably I can come close to that as well.

On the business of the importance . . .

Mr. Beatty: Including, Mr. Finch, federal data banks?

Mr. Finch: I guess we are—off the record or . . . we are on the record, are we not? I guess no comment.

Mr. Rous: On the record, there are government data banks within Canada that we know we can walk right into. That much we will put on the record.

Mr. Beatty: Let me just pursue this, if I may: Are you aware of any instance where federal data banks have been violated and where the data base has been damaged or where personal information relating to individuals has been taken by unauthorized people?

Mr. Rous: That is another one that I would prefer not to answer.

Mr. Finch: I would like to draw an analogy: Certainly we have had some first-hand experience with provincial computer installations, and I leave it to your judgment as to whether the federal systems are better protected or not.

Mr. Rous: I can perhaps tell you an illustrative story, and this is part of the public record. About two years ago, the Auditor General criticized the Department of National Revenue. The criticism was that while they did have back-up copies of the taxpayer master files, those back-up copies were located in the same building, which meant that had there been a massive explosion which destroyed the taxation data centre in south Ottawa, all taxpayer files would have been lost—all taxpayer files. If we consider that as one—granted, an anecdotal, not necessarily a representative—example of the type of omission that is very easy for the custodian of the data centre to make, then perhaps you have some idea that there may be other dangers there as well.

[Traduction]

presque tous les jeunes aujourd'hui savent quoi faire devant un terminal. La mystique de l'ordinateur commence à disparaître. Beaucoup craignent que nous ne soyons en train d'engendrer une génération de bandits de l'informatique. Je ne vois pas les choses de cette façon car je pense que nous aurons toujours une frange criminelle dans notre société et une meilleure connaissance des machines que nous utilisons nous permettra de mieux contrer ces éléments.

Le nombre de systèmes auxquels on peut avoir accès est énorme. J'ai visité récemment, en une seule soirée, quatre installations informatiques et dans trois cas, j'ai pu me rendre directement dans la salle des machines au nez et à la barbe des gardiens et en déjouant le système de sécurité sans user d'aucune violence. Je reconnais que dans un cas, j'ai donné un nom fictif à l'entrée et je me suis rendu à un étage différent de celui où j'étais censé aller. Donc, sur le plan professionnel, nous avons une lourde tâche d'éducation à faire auprès de nos clients. L'accès au système . . . Je vous fais le pari qu'aucun système du pays ne pourrait résister à mon partenaire Rous ici présent, et il n'y a pas beaucoup qui me résisteraient personnellement.

Pour ce qui est de l'importance . . .

M. Beatty: Y compris les banques de données fédérales, monsieur Finch.

M. Finch: Est-ce que l'on nous enregistre? Si oui, pas de commentaires.

M. Rous: Je puis dire officiellement qu'il existe des banques de données du gouvernement qui sont accessibles sans aucune difficulté.

M. Beatty: Permettez-moi d'insister: avez-vous connaissance de banques de données fédérales qui auraient été violées ou dont la mémoire aurait été effacée ou dont des données d'ordre personnel seraient tombées entre les mains de personnes non autorisées?

M. Rous: Là encore, je préfère ne pas répondre.

M. Finch: Essayons donc une analogie: nous avons une expérience de première main des systèmes informatiques provinciaux et j'aimerais savoir comment ils se comparent aux systèmes fédéraux, s'ils sont mieux protégés ou non?

M. Rous: À titre d'illustration, je peux vous conter une anecdote qui est déjà connue. Il y a deux ans environ, le vérificateur général a critiqué le ministère du Revenu national parce que celui-ci entreposait dans le même bâtiment les copies en double des dossiers des contribuables, si bien que si une explosion massive avait détruit le centre des données fiscales d'Ottawa, tous les dossiers des contribuables auraient été perdus. Ce n'est pas nécessairement un exemple représentatif mais c'est le genre d'erreur qui se fait très souvent. Cela vous donne une idée des nombreux dangers auxquels on s'expose.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Your complaint there is that they did not have a back-up system.

Mr. Rous: They did not have any other files away from the data centre. It is easy to replace a computer. If my computer starts to smoke, the way an oven sometimes does, and the whole thing blows up, I can phone up my supplier and have a new computer in a few weeks. But if all my master files go up in smoke and I do not have another copy somewhere else, how do I recover? I cannot. What it means is that all your tax information for the last few years would have been lost and the taxation people would not even know that any of us existed. They would be starting over from scratch, trying to figure out who the taxpayers were, to know whether or not we had paid our taxes.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): I am not clear on this. When you are talking about a back-up system, are you talking about a back-up computer or a...

Mr. Rous: No.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): —back-up set of data?

Mr. Rous: A back-up set of data, in this case. They had one set of data sort of with the machine, they had another set of data down in the basement of the building. Ideally, the standard rule that all our clients follow, and almost everybody follows, is that you have another set of that data separated by several miles, just in case you have something like a Mississauga train disaster. According to the Auditor General, taxation had not done that. That is a fairly fundamental precaution. If it is easy enough to slip up—and I am not really criticizing Taxation, I am pointing out that it is very easy to slip up on some of these precautions—if you can slip up on one like that, I think we can safely presume it is possible to slip up on others.

Mr. Beatty: In your experience, most of the instances you have cited have involved a lack of physical security, as opposed to technological security.

• 1630

The Dalton School case would be an exception to that.

What you were referring to with the taxation data is a case of physical security. Mr. Finch indicated when he visited various data centres that there was a problem of physical security. Where you have been dealing with private sector clients, has it been the case that you generally found that their greatest problems are of physical security as opposed to technological security around the computer?

Mr. Finch: It is a combination. I think it is both. I think the point I was trying to make was that there was a lack of physical security and that in turn gave us access to the terminals that were on line. In other words, as opposed to having to dial up and come into that system, which might not have been available to us, we were able to easily reach a

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Votre reproche ici est qu'il n'y avait pas de système de secours.

M. Rous: Les archives étaient entreposées dans le même bâtiment. Il est facile de remplacer un ordinateur. S'il se met à fumer et à exploser comme cela arrive parfois, je n'ai qu'à appeler mon fournisseur et il m'en installe un nouveau dans l'espace de quelques semaines. Par contre, si toutes mes archives partent en fumée, et que je n'aie pas de doubles entreposés ailleurs, qu'est-ce qu'il me reste? Rien. Cela signifie que toutes les données fiscales des dernières années auraient été perdues et le fisc ne saurait même pas que nous existons. Il devrait repartir de zéro, essayer de trouver qui étaient les contribuables, s'ils ont payé des impôts ou non, etc.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je ne comprends pas très bien. Lorsque vous parlez d'un système de secours, parlez-vous d'un ordinateur de secours ou bien...

M. Rous: Non.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): De données de secours?

M. Rous: Dans ce cas, d'archives de secours. Le ministère avait un jeu de données en mémoire dans la machine, et un autre jeu entreposé dans la cave. La règle normale, que presque tous nos clients suivent, est d'entreposer un autre jeu de données à plusieurs milles de distance, au cas où il se produit une grande catastrophe comme par exemple le désastre ferroviaire de Mississauga. Selon le vérificateur général, le ministère du Revenu avait négligé de le faire. C'est pourtant une précaution très fondamentale. Si l'on commet des erreurs aussi évidentes—et je ne le dis pas cela pour critiquer l'impôt, mais pour montrer combien il est facile de faire des erreurs—on peut alors conclure que beaucoup d'autres, moins évidentes, se commettent aussi.

M. Beatty: Dans la plupart des cas que vous avez cités, il s'agissait d'un manque de sécurité matérielle plutôt que de sécurité technologique.

Le cas de l'école Dalton est une exception.

Dans le cas des données fiscales, il s'agit bien d'un problème de sécurité matérielle. M. Finch nous a parlé d'un problème de sécurité matérielle dans les divers centres de données qu'il a visités. Est-ce la même chose chez vos clients du secteur privé ou bien est-ce que leur problème touche plutôt à la sécurité technologique?

M. Finch: C'est une combinaison des deux. L'absence de sécurité matérielle nous permettrait d'accéder aux terminaux, qui eux-mêmes donnent accès à la mémoire. Plutôt que d'accéder par branchement téléphonique, ce qui aurait peut-être été impossible, nous aurions été en mesure de pénétrer dans les locaux et de manipuler le terminal et je suis certain que nous aurions pu ainsi «casser le système».

[Texte]

terminal, and I have every confidence that we could have breached the system with that.

Mr. Rous: The other point that goes with that, though, is that physical security has been well understood for many, many years and you can safely assume that somebody who has ignored physical security has probably ignored a lot of aspects of far more technical, leading-edge, logical security as well.

Mr. Finch: I would like to come back to two points. One was the severity or the occurrence of these incidents in business. I would like to point out the dependence of some life-saving types of systems: in the medical area, patient monitoring; if you like, a system as simple as aircraft loading, where any tampering with the system can affect lives. This does not affect a person's bank account necessarily. We are increasing our use of computers in these areas at, really, a remarkable and an alarming rate. This is certainly the use of computers. It may not be business; it may be government or agencies or some quasi-organization like that, but certainly we are more dependent. We are dependent, if you like, in Toronto on our traffic control system, and all of these have very grave consequences.

On the number of incidents, I would like to relate an experience that we had, actually about a year and a half ago, where the director of security of a very large organization called me to sit down and have a discussion on the statistics. He had debunked the Donn Parker curves and he had decided that the computer abuse was a flash in the pan that started in the early 1970s, grew to some kind of crest in 1978 and was now on the decline. This was back about a year and a half ago.

Mr. Beatty: That is the Peter Watkins thesis?

Mr. Finch: I guess so, yes. Yes. In actual fact, of course, there is always a delay to when the incidents are discovered and reported. I am not aware that there has been, in fact, any decline in the actual occurrences. Certainly, in our experience, we find that before being retained on an assignment there is a certain amount of carefulness in discussing problems; but, once we are engaged and have the opportunity for the employees of the company to speak frankly with us, suddenly all kinds of occurrences are brought to our attention in order that we may understand some of the concerns and actually why we have been called in.

Now, some of this could be put down to employee errors and omissions, but often it could be classed as embezzlement. In some cases it is unknown; there is just a mysterious disappearance of some asset on the books, which may not be money itself but can be transferred into money.

So, in my mind, there is no indication that this is a declining problem. I think that in fact it is an increasing one, and I think that computer crimes will continue to be more and more sophisticated.

Mr. Rous: We are not, by the way, trying to debunk Peter Watkins' debunking. We know the article and what he said is factually true. What we are saying, though, is that, firstly, we have shown that it is so easy and so possible and the potential

[Traduction]

M. Rous: Ce qui est révélateur là-dedans, c'est que la sécurité matérielle est un facteur que l'on connaît bien depuis de nombreuses années et celui qui ignore une nécessité aussi évidente, ignore probablement aussi un grand nombre d'aspects beaucoup plus techniques, propres aux ordinateurs.

M. Finch: J'aimerais revenir sur deux points. Le premier est la gravité des incidents qui se sont produits dans ce secteur. Il faut souligner la dépendance de certains systèmes, notamment dans le domaine médical, qui mettent notre vie en jeu: le monitoring des malades, par exemple, ou en aéronautique, le chargement des avions, où toute interférence peut mettre en danger des vies. Ce n'est pas uniquement le compte en banque des gens qui est en cause. On a recours de plus en plus à l'informatique dans ces domaines, et le rythme s'accélère de façon presque alarmante. Les risques n'existent pas que pour les établissements commerciaux, les gouvernements et les organismes publics sont également de plus en plus dépendants de l'informatique. À Toronto, beaucoup dépend du système de régulation de la circulation dont la panne ou le mauvais fonctionnement peut avoir des conséquences très graves.

En ce qui concerne le nombre des incidents, j'aimerais vous relater une expérience que nous avons eue il y a 18 mois. Le directeur de la sécurité d'une très grande entreprise m'a appelé pour discuter des statistiques. Il était tombé sur les courbes Donn Parker et avait conclu que la criminalité informatique avait fait une apparition soudaine au début des années 1970, avait atteint l'apogée en 1978 et était maintenant sur le déclin. C'était il y a environ 18 mois.

M. Beatty: Est-ce que c'est la thèse de Peter Watkins?

M. Finch: Je pense que oui. En fait, il y a toujours un retard entre le moment où l'on découvre les incidents et celui où on les déclare. À ma connaissance, il n'y a pas eu vraiment un recul de l'incidence. Notre expérience montre que, en début de mission, les gens hésitent à nous parler franchement mais une fois que nous sommes lancés, que les employés de l'entreprise commencent à nous parler en toute franchise, alors ils nous signalent toutes sortes d'incidents qui se sont produits par le passé, afin de bien nous faire comprendre la nature des problèmes et la raison pour laquelle on fait appel à nous.

Souvent il s'agit simplement d'erreurs ou d'omissions de la part des employés, mais très souvent également on pourrait parler d'escroquerie. Dans certains cas, on ne sait pas comment elle a été réalisée, on constate simplement la disparition mystérieuse des livres de tel ou tel avoir, qui n'est pas nécessairement de l'argent, mais qui peut être converti en argent.

Rien n'indique donc, à nos yeux, que le problème diminue. Au contraire, nous pensons qu'il est en augmentation et que la criminalité informatique va se poursuivre et devenir de plus en plus sophistiquée.

M. Rous: Nous ne voulons nullement démolir la théorie de Peter Watkins. Nous connaissons son article et les faits qu'il énonce sont vrais. Ce que nous disons, c'est en premier lieu que le potentiel est si énorme et que même s'il n'y avait jamais eu

[Text]

is so great that, even if there had never been one major computer crime, all of the little Dalton School cases and U. of A. cases and New Brunswick fishery cases prove that there is still a requirement to protect; and, secondly, we know from the anecdotal evidence that we get on our assignments that the problem does exist out there. The statistics: Peter Watkins is dead correct. The statistics are worth virtually nothing; do not trust them for anything. The problem though is real.

• 1635

Mr. Beatty: Can we return to your proposals which Mr. Finch made before on how to deal with this because, in wrestling with the bill myself, I found there are several different approaches one can take to deal with the problem. I think the Department of Justice has properly pointed out that the bill creates problems in some areas and that virtually any solution you try to put into place has limitations to it and, in some ways, may complicate it. For example, by treating data stored in a computer differently from manually-stored data, you could make it an offence to take information from a computer when it would have been perfectly appropriate to take it from a file-folder. And the argument has been made that it is improper to take any action on that ground. Now you are saying that you want to deal with the offence of the action as opposed to getting too technical in trying to define terms and getting too deeply into the technology. What exactly have you in mind? What would be the crime?

Mr. Finch: One of the problems which I think does not need explaining is that, when your data is stolen you have still got it. I think we all understand what I mean by that. We have a copy of it. And we do not often know that it has even been copied. The difference I would like to distinguish between in taking a piece of paper from a filing cabinet, which you say is right, and taking the information from a computer is very much like the example I gave where someone says: Well, the information in the computer is available to you. It is in the public domain. You can have it. The question is, however: How did you get it?

With the computer the case is different in every instance, but we have machines worth on the small side, say, \$10,000 but, on the high side, \$10 million, where someone in an unauthorized fashion is travelling through your corridors. In business we do not want that. We know we have a problem. We have a very large hotel, and we just do not want hoboes and transients and unknown persons not known to us, walking through those halls. We have too much at stake as they go by the rooms. And I think it is that essence of trespass, if you like.

Now I am not a lawyer and I cannot express myself as a lawyer might in looking at the actual wording of the legislation. But the point I have made, I think, is that there is a sense of permissiveness being condoned in many sectors that it is all right to walk through that hotel. It is a public area. In business that is rarely the case. In business in nearly every case the computer is privately owned; the data is privately generated and owned.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I do not know that I could share your analogy

[Translation]

un seul grand délit informatique commis, tous ces petits incidents genre école Dalton etc., montrent la nécessité de la protection; en deuxième lieu, que les indications anecdotiques que nous recueillons dans nos missions montrent bien qu'il s'agit d'un problème réel. Pour ce qui est des statistiques, Peter Watkins a tout à fait raison. Les statistiques ne valent pratiquement rien, ne vous y fiez pas. Le problème existe.

M. Beatty: Pourrions-nous revenir sur les propositions que M. Finch a faites quant aux remèdes à apporter, car je vois moi-même plusieurs approches possibles. Le ministère de la Justice a bien fait ressortir que le projet de loi crée des problèmes dans certains domaines et que toute solution que l'on puisse imaginer présente des limitations et risque parfois même de compliquer le problème. Par exemple, en faisant la distinction entre les données informatiques et les archives matérielles, on risque de faire un délit du retrait de données informatiques alors qu'il aurait été parfaitement licite de les tirer d'un dossier cartonné. On fait donc valoir que la forme sous laquelle se présentent les données ne peut être un critère. Vous dites vous-même qu'il faut considérer le caractère délictuel de l'acte matériel, plutôt que le contenu des données, ce qui poserait des problèmes de définition et présenterait des difficultés techniques. A quoi songez-vous exactement? Comment définiriez-vous le délit?

M. Finch: L'un des problèmes, qui se passe d'explications, est que lorsqu'on vous vole vos données, vous continuez quand même à les posséder. Tout le monde le comprend. Les données subsistent et bien souvent on ne se rend même pas compte qu'elles ont été copiées. Il faut distinguer entre le fait de prendre connaissance d'un dossier, ce qui peut être parfaitement licite, et celui de retirer des données d'un ordinateur. Ces données peuvent être dans le domaine public, c'est-à-dire que tout le monde peut y avoir accès, mais la question qui se pose est de savoir par quel moyen.

Chaque cas est un cas particulier, mais nous avons des machines qui valent de \$10,000 à 10 millions de dollars et on ne peut pas laisser n'importe qui se promener dans les couloirs. Ce n'est pas souhaitable et le secteur privé sait qu'il y a un problème. Prenez un grand hôtel, vous n'allez pas laisser n'importe quel vagabond ou n'importe quel inconnu se promener dans les couloirs car le risque est trop grand. C'est la notion d'intrusion qui doit jouer ici.

Je ne suis pas juriste et je ne saurais pas comment m'expliquer en langage juridique. Il y a un certain laisser-aller dans beaucoup de secteurs, on peut considérer que n'importe qui peut se promener dans un hôtel puisque c'est un lieu public. Mais c'est rarement le cas dans les entreprises où presque toujours l'ordinateur est une propriété privée, de même que les données qu'il renferme.

Le président suppléant (M. Robinson (Etobicoke-Lakeshore)): Je ne peux pas accepter votre analogie parce que même

[Texte]

because I think if you were looking at it from a legal point of view that, even in a hotel, there are certain areas considered to be public and certain areas considered to be private, even if it is private to those who have rooms in the hotel. Yet, there is a commonality of areas by walking into the lobby, say, so I would be rather careful in choosing that kind of analogy to apply to this kind of situation.

Mr. Rous: But if it were a private office building, we could stop the person coming in at all.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You might do that too. But I want to come back to something else. You seem to be sort of concerned that we are not dealing with an absolute. It seems to me that the only two absolutes that I know of are death and taxes. And apart from that . . .

Mr. Beatty: We are working on death though.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): That is right. We are trying to prolong people's lives to maybe eliminate that aspect of it, but the taxes would still continue. There are no absolutes. We know that. It is a question of what can we do by way of some safeguards, even if you say, Well, Fort Knox is loaded with gold. But, you know, it could be taken away. It would be a tremendous task to do it.

• 1640

So what we are really looking at, even with the legislation, is to see it from the point of view of the kinds of safeguards we can build into the system that are going to either make it so difficult to deal with or the consequences of it are going to be so difficult that it will deter people from getting involved. And I wondered, since you people have been involved in this for some 25 years and more, what sort of fail-safe provisions are you suggesting or have been developed; or do we not have any? And if we do not have any, why have we or you been so dilatory in not providing them and coming to this kind of conclusion long before this?

Mr. Rous: There are no fail-safe provisions possible today. We can all hypothesize about a fool-proof computer some time in the future.

I guess what we are talking about here is not a question of absolutes; what we are really addressing is the focus of legislation. We are not suggesting that you come up with an absolute; we are suggesting that it is the activity that should be the focus as opposed to the consequences of the activity or the object of the activity. In other words, what we are concerned about is that unauthorized access and use of a computer should be the offence as opposed to theft of data, copying of data, selling of a program, as opposed to the technical definition of what the computer is that you are accessing, etc. We are not asking for absolutes in legislation when we cannot have absolutes on the computer side.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You know, I have visited several companies since I got involved in this committee to try to find out from them what sort of security they had for their data banks, their

[Traduction]

dans un hôtel, du point de vue juridique, certains secteurs sont considérés comme publics et d'autres comme privés et l'accès en est limité aux clients. D'autres secteurs sont publics, comme le foyer par exemple, si bien qu'il faut utiliser ce genre de comparaison avec beaucoup de prudence.

M. Rous: Oui, mais s'il s'agit de bureaux privés, on peut en interdire l'accès à qui l'on veut.

Le président suppléant (M. Robinson Etobicoke—Lakeshore): Certainement, mais j'aimerais revenir sur autre chose. Vous semblez déplorer qu'il n'y ait pas d'absolu. Il me semble que les deux seuls absolus sont la mort et les impôts. À part cela . . .

M. Beatty: Nous commençons à nous attaquer aussi à la mort.

Le président suppléant (M. Robinson Etobicoke—Lakeshore): Oui, et nous essayons de prolonger la vie des gens mais les impôts, eux, ne disparaîtront pas. Il n'y a pas d'absolu, et nous le savons. Il s'agit de savoir jusqu'où l'on peut se protéger. Fort Knox est rempli d'or et il serait possible de le voler. Ce serait une tâche formidable mais pas impossible.

Donc, même la loi devra veiller à ce que des dispositifs de protection soient intégrés au système pour empêcher toute intrusion ou à ce que le maniement en soit si difficile qu'il constituerait une importante force de dissuasion. Puisque ces techniques n'ont pas de secret pour vous depuis vingt-cinq ans et plus, je me demande quelle sorte de dispositifs de protection ont été intégrés au système. Quelles garanties proposez-vous si nous avons le choix? Et si ces garanties n'existaient pas, pourquoi vous a-t-il fallu tant de temps pour en arriver à cette conclusion?

M. Rous: Il n'existe pour le moment aucune protection infaillible. Nous pouvons tous rêver d'un ordinateur à tout épreuve pour l'avenir.

Nous ne parlons pas ici d'une question d'absolu mais plutôt de l'orientation à donner au texte législatif. Nous voulons que la loi soit axée sur l'acte lui-même et non pas sur les conséquences ou sur l'objet de cet acte. En d'autres termes, nous voudrions que l'infraction porte sur l'utilisation indue d'un ordinateur et non pas sur le vol de données, la reproduction de données, la vente d'un programme, et sur la définition technique de l'ordinateur violé, etc. Rien n'est à tout épreuve du côté ordinateurs et par conséquent, nous ne pouvons pas vous demander une loi à toute épreuve non plus.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Depuis que je fais partie de ce Comité, j'ai visité plusieurs sociétés pour essayer de savoir quel système de sécurité était intégré à leurs banques de données, quelles

[Text]

formulas for their products and all kinds of things of this nature, and they indicate to me that as far as they are concerned they have tremendous in-house control. You talk about this in-house control; well, they consider they have it. They have educated their employees about it; they have all sorts of systems set up whereby only certain people are authorized to go into certain rooms; there are only certain people who are authorized to have certain access to data in terminals and so on, and they figure they have covered this completely.

When I asked one company in particular what safeguards they had towards somebody getting into their data bank from the outside, not the in-house, this was something that is foreign to them completely. They have no idea that this can be done, and this is the kind of thing that I think you people are telling us about and that the public should be aware of, and these companies and so on should be aware of; that they are not home-free just because they have put everything in their computer. Maybe they should be locking their formulas up in the safe and locking other information up in the safe and not leaving it in a computer bank.

And so, is there any way you can put something on and take it off and keep it in a different storage pattern, or some different way or some other method, rather than leaving it for somebody to dabble with; or can you take parts of it out and remove the significant parts? You know, what are you people looking at by way of safeguards? You must be looking at something, because how can these companies properly protect themselves? Even if they have tremendous security in-house, how do they protect themselves from somebody taking this stuff from outside?

Mr. Rous: That is easy; but as you said they have to be aware that it happens, and that is why we said right at the beginning that we believe that legislators not only in providing deterrents will also provide education and public awareness; and we believe that is a very important role. We can help a company prevent an outsider from getting any meaningful data if that company is aware of the fact that they have a problem in the first place.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): Supposing they are not aware of it?

Mr. Rous: Then there is nothing that either you or we can do.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have used two terms—prevention and deterrents—and I do not know whether you mean prevention versus deterrents or whether you are talking about prevention and deterrents; and if you are talking about prevention you are not talking about legislation per se, you are talking about the computer field itself.

Mr. Rous: Technological prevention, yes.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): Yes, that kind of thing; but in the deterrents, you feel that the deterrence is only in legislation. Is that fair?

[Translation]

formules elles appliquaient à leurs produits et ainsi de suite; elles m'ont toutes dit que le contrôle interne était important. Vous en avez parlé et ces sociétés estiment qu'elles disposent déjà de ce contrôle. Elles en ont parlé à leurs employés, elles ont mis sur pied toutes sortes de systèmes selon lesquels seules certaines personnes sont autorisées à entrer dans certaines pièces, à avoir accès à certaines données informatiques, et ainsi de suite, et elles estiment que leur système de sécurité est à toute épreuve.

Lorsque j'ai demandé à une société quel système de sécurité elle avait mis en place pour empêcher quelqu'un de l'extérieur d'utiliser ses ordinateurs, elle n'y avait même pas pensé. Ces sociétés ne savent pas que cela peut se faire et c'est, je crois, ce que vous êtes en train de nous dire; le public devra en être conscient ainsi que toutes ces sociétés; elles ne devraient pas penser qu'elles sont à l'abri de tout simplement parce qu'elles ont intégré toutes leurs données dans leurs ordinateurs. Elles devraient peut-être même songer à enfermer leurs formules dans un coffre-fort ainsi que toute autre information délicate et non pas les laisser dans une banque de données.

Donc, peut-on mettre des données dans un ordinateur, les retirer et les garder sous une forme différente au lieu de les laisser dans un ordinateur et permettre ainsi à n'importe qui de s'en servir? Ou alors, peut-on en retirer certaines parties? Quels dispositifs de sécurité envisagiez-vous? Vous devez envisager quelque chose car, dans le cas contraire, comment ces sociétés pourraient-elles se protéger? Même si leur sécurité interne est pratiquement à toute épreuve, comment peuvent-elles se protéger de quelqu'un venant de l'extérieur?

M. Rous: C'est facile, mais comme vous l'avez dit, elles doivent en être conscientes et c'est la raison pour laquelle nous avons dit dès le début que la loi devrait non seulement comporter des dispositions dissuasives mais également contribuer à la conscientisation et la sensibilisation du public au problème; nous pensons que c'est là un rôle très important. Nous pouvons aider une société à empêcher un intrus venant de l'extérieur d'obtenir des données importantes à condition que cette société sache qu'elle a un problème dans ce domaine.

Le président suppléant (M. Robinson (Etobicoke... Lakeshore)): Et si elles n'en sont pas conscientes?

M. Rous: Dans ce cas, vous et moi ne pouvons rien faire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé de dispositions préventives et de dispositions dissuasives, mais je ne sais pas si vous opposez ces deux termes ou non. Et si vous parlez de dispositions préventives, vous ne parlez pas de la loi-même, mais plutôt du domaine informatique.

M. Rous: Oui, il s'agit de dispositions préventives d'ordre technologique.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui, mais pour ce qui est des dispositions

[Texte]

Mr. Rous: I believe so, because without the legislation, if somebody bypasses whatever technological measures I have put in or have not put in, they manage to bypass them and do significant harm. Without legislation, all I can do is shrug and say, well, I will try and do better next time.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): If you are looking at it from the point of view of the Criminal Code, or would you consider there might be a special act? As you may or may not appreciate, any federal statute has criminal connotations by way of penalties, so that even if there was a computer act set up and there were penalty provisions in it, it would be criminal in nature as far as that is concerned. You would probably have a record; or at least, there would be something on your record if you were convicted of this kind of crime.

• 1645

Do you have any suggestions to make with regard to this piece of legislation, which is the subject of our whole discussion on computer crime, or any special suggestions to make with regard to changes in the Criminal Code, additional sections that should be added or wording that should be used? Do you have any sample suggestions to bring to our attention? Have you looked at the structure and the presentation of a bill that would cover the kind of thing that in your mind would deal with the whole question of deterrence?

Mr. Rous: We have provided input to the Department of Justice over the last little while as to where we think the legislation should be going. That input, I believe, is on the record with Justice themselves.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Finch, you have indicated there are problems now with employee screening because of the human rights legislation, provincially and federally and so on. Do you have any suggestions to make as to how this legislation should be changed? Specifically, if it happens to be someone who is applying for a job in running a computer, a computer programmer or whatever it may be, do you have any specific suggestions there?

Mr. Finch: I think there is a need for a greater screening of the people who are going to take responsible positions in a computer operation. I believe many of the personnel departments feel it is a screen they are not allowed to make.

We have resorted to some other techniques. We sometimes look at bonding and that sort of thing, where an independent organization, through methods of their own, will go deeper into a person's character. But there is no question, often after some crime or some incident has occurred, when the person has been looked at a little more closely, it has been obvious this is just

[Traduction]

dissuasives, vous pensez que cette dissuasion ne peut venir que de la loi. Est-ce juste?

M. Rous: Je crois que oui, car sans texte législatif, si un individu arrive à surmonter les obstacles technologiques que j'ai intégrés ou non au système, cet individu peut me faire un tort important. Sans texte législatif, tout ce que je peux faire, c'est hausser les épaules et me dire que je ferai davantage attention la prochaine fois.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Pensez-vous que le Code criminel devrait être modifié ou qu'une loi spéciale devrait être adoptée? Peut-être le savez-vous, mais toute loi fédérale comporte des dispositions d'ordre pénal puisqu'on impose des amendes; par conséquent, même si une loi sur les ordinateurs était adoptée et que cette dernière prévoit des amendes, elle serait de nature pénale. Vous auriez vraisemblablement un casier judiciaire ou du moins, une mention serait portée sur votre casier si vous étiez condamné pour ce genre de délit.

Avez-vous des suggestions à faire quant aux dispositions que devrait renfermer ce texte législatif, qui fait l'objet de toute notre discussion sur le cambriolage informatique? Ou avez-vous des propositions spéciales à formuler quant aux modifications qui pourraient être apportées au Code criminel, quant aux articles complémentaires qui devraient y être ajoutés ou quant au libellé qui devrait être adopté? Avez-vous des suggestions types à nous faire? Vous êtes-vous penché sur les dispositions que pourrait comporter un projet de loi et qui porteraient sur toute la question des moyens de dissuasion?

M. Rous: Depuis quelque temps, nous collaborons à ce sujet avec le ministère de la Justice et je pense donc que vous pouvez vous adresser à ce dernier.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Finch, vous nous avez dit tout à l'heure que des problèmes se posaient maintenant au niveau de la sélection des employés en raison de la Loi sur les droits de la personne, tant à l'échelle provinciale que fédérale. Avez-vous des suggestions à faire quant aux modifications qui pourraient être apportées à ce texte législatif? Plus précisément, s'il s'agit d'un individu qui brigue un poste de programmeur ou un autre poste dans le domaine informatique, avez-vous des suggestions précises à faire?

M. Finch: Je pense qu'il faut effectivement passer au peigne fin les individus qui sont appelés à exercer des fonctions importantes au sein d'une société d'informatique. Je crois que de nombreux départements du personnel pensent qu'ils ne sont pas autorisés à soumettre les candidats à ce procédé de sélection.

Nous avons eu recours à d'autres techniques, comme le cautionnement par exemple. Parfois, une entreprise indépendante, par des méthodes qui lui sont propres, peut faire une étude approfondie du caractère du candidat. Mais en général, lorsqu'un délit ou un incident quelconque a eu lieu, et que l'individu en question a été étudié de manière plus approfondie,

[Text]

another succession in a series of events in that person's career, all of which were offensive or destructive.

I have a little trouble expressing myself legally, but I would like to address your question of whether or not there is a problem. We are dealing with a people problem. I know it is against the law to kill people, and this is not a question of capital punishment. If I kill someone and I am found doing it, I know I am going to be put away for a long time; and therefore, I do not want to be put away for a long time and I do not want to kill anyone.

At the same time, we have mentioned this rather slack attitude about computers, that it is fun to break a computer. I would like you to examine the scenario of an organization that is conscious of computer security, that has manuals describing the proper procedures for its employees, that takes every effort to train those employees, that has staff assigned to computer security. I would like to laughingly, or somewhat in jest, describe to you the computer recovery program that was locked up in the vault and took two weeks to get out, like some of the procedural problems we fall into sometimes. I am thinking of one organization with all this in place, where because of human nature, the prescribed procedures were, in fact, not carried out.

Security is a burden for companies in most cases. It adds an extra step—make sure the door is locked behind you; make sure you sign off your terminal when you leave it—although you might speak to a very senior person who says: Yes, we are doing everything we can to secure our system. He is right; he is, and I mentioned this in my talk. We are doing everything we can. Nonetheless, because of human nature, we are still exposed.

At that point, I think the majority of the citizens are deterred if they know there is a heavy consequence of abusing the computer system. This, of course, will not deter perhaps a hardened criminal. Perhaps he sees that as the challenge and the opportunity. But it will deter a lot of people.

[Translation]

on se rend compte qu'il ne s'agit que d'un autre incident qui vient s'ajouter à toute une succession d'événements qui ont eu lieu dans la carrière de cet individu, dont tous étaient nuisibles ou destructifs.

J'ai quelques difficultés à m'exprimer en termes juridiques, mais je voudrais aborder la question de savoir si un problème existe ou non. Il s'agit d'un problème de personnes. Je sais qu'il est illégal d'assassiner son prochain et il ne s'agit pas ici d'une question de peine capitale. Si j'assassine quelqu'un et que je sois déclaré coupable, je sais que l'on va m'emprisonner pendant longtemps; par conséquent, je ne le veux pas, pas plus que je ne veux tuer quelqu'un.

Mais nous avons parlé tout à l'heure de ce laisser-aller à l'égard des ordinateurs, à savoir que voler les données d'un ordinateur constitue un amusement. Prenons une entreprise qui a conscience du problème de sécurité, qui possède des manuels décrivant les procédures à suivre à l'intention de ses employés et qui ne ménage pas ses efforts pour former ses employés et dont certains employés ont la charge du système de sécurité. Je pourrais aussi vous citer l'exemple un peu amusant de la fois où nous avons mis deux semaines à récupérer notre programme-clé qui avait été enfoncé dans le coffre-fort. Je pense à une entreprise qui possédait un très bon système de sécurité, mais qui ne le mettait pas en oeuvre en raison de la nature même de l'homme.

Dans la plupart des cas, la sécurité constitue un fardeau pour les sociétés. C'est un problème supplémentaire, il faut veiller à ce que la porte soit verrouillée, à ce que le terminal ne soit plus en état de marche lorsque vous n'en avez plus besoin et certains vous diront d'ailleurs qu'ils font tout pour que leur système soit le plus sûr possible. Ils ont raison et j'en ai déjà parlé. Nous faisons tout ce que nous pouvons dans ce domaine. Néanmoins, les risques demeurent en raison de la nature humaine.

Je crois d'ailleurs que la majorité des gens hésiteraient beaucoup à saboter un ordinateur s'ils savaient que les conséquences en seraient lourdes. Évidemment, cela ne dissuaderait pas un criminel endurci. Il y voit peut-être un défi, mais la plupart des gens hésiteraient beaucoup à le faire.

• 1650

It is when people start fooling around with the systems and talking to each other that they share information on how to access somebody else's files, not their own. I think if you look at an organization and talk at the top of it, you will find a rather managerial attitude that says: we are doing everything we can, considering our means. Then, I think, as you come down into a more operational area, the person will say: we have a number of exposures; we know what those exposures are and we are watching those exposures very carefully. Then as you come down onto an operational level, you will find that in practice the place is wide open. When I say wide open, I refer either to physical doors or to terminals being left available for a reasonably intelligent person to access.

Le problème se produit quand les gens se mettent à tripoter les systèmes et à se parler entre eux et qu'ils partagent des renseignements sur la façon d'avoir accès aux programmes d'un tiers et non pas des leurs. Je crois que si vous parlez avec les dirigeants d'une entreprise, vous entendrez ceci: Nous faisons tout ce que nous pouvons, en fonction de nos moyens. Ensuite, si vous vous adressez aux cadres un peu plus spécialisés, ils vous diront: Nous avons un certain nombre de points faibles, nous savons quels sont ces points faibles et nous faisons très attention. Puis, lorsque vous parlez avec ceux-là même qui exploitent le système, vous constatez qu'en fait, on peut y entrer comme dans un moulin. Quand je dis ceci, je fais allusion soit aux portes qui sont carrément ouvertes soit aux terminaux auxquels pourrait accéder une personne relativement intelligente.

[Texte]

This is our problem. We spend our time really as catalysts, telling the people what they already know, encouraging them to get on a new program of safety and security. You see this in plants all the time with dangerous equipment, you know: let us not have any lost hours this month; let us have no violations this month. So there is a certain amount we can do that way. But the other side that always comes out is the frustration, the frustration that we find within the security organizations or the security office of large corporations where offences have occurred. They have taken disciplinary action—the employee may have been fired—but they often shrug their shoulders or they simply give up at the thought of prosecution because they know the effort and the energy is probably not going to be worth while to them. Also they know it will bring them a lot of bad press. We still see a lot of this. None of us likes to admit that we are vulnerable.

As a matter of fact, one of the problems we have is that many people feel that if you talk about the security precautions you are taking, you are telling people how to break them, and I disagree with this. I think many of our companies do not make enough of an issue that they have in fact taken precautions so that their customers and their employees and the public have a greater confidence. It is very much a people problem, and this deterrent is very much an important part of how the staff and outsiders conduct themselves.

I am sure that just by the nature of the company, a person wishing to attack a machine would set his priorities. You know companies that are managed by hard people, tough people, and companies that are soft. It is the same with a boxer, I guess. It becomes a competition, and there is no framework out there that overall says: this is wrong, do not do it.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): I get the impression from what you have said that passing a statute or amendments to the Criminal Code would in effect be a deterrent in itself, but you really have to be looking in terms of the penalty for the theft of computer data. I do not know what kind of sentencing principles you would use in something like this. I suppose once again the absolute is that if a person is caught committing an offence, if there is such an offence as computer theft, they are put away for life so they cannot do it again. That is the absolute, I suppose, but how do you show this as a deterrent? If the value that is in computer theft itself is so tremendous, it is almost beyond one's comprehension if you are looking at it in a quantum of dollars and cents. Then really the enticement to continue into crime is still there, and as one of you indicated by way of an illustration, well, you have 60 days for stealing \$800,000 and you serve 40 days; but, you know, really, if you are talking about stealing \$250 million or billion by the same process and you get life, what is that? You consider the odds of being caught in the first place.

As a lawyer, and doing some criminal law, I never ever met anybody in my whole practice who expected to be caught when

[Traduction]

Voilà où réside notre problème. Nous sommes un peu des catalyseurs, nous disons aux gens ce qu'ils savent déjà, nous les encourageons à adopter un nouveau programme de sécurité. On constate la même chose tout le temps dans toutes les sociétés possédant du matériel dangereux, qui se disent: Ce mois-ci veillons à ce qu'aucune heure ne soit perdue, à ce qu'aucune infraction ne soit perpétrée. Nous pouvons donc agir dans ce sens. Mais il faut également tenir compte de la frustration, du découragement propre aux bureaux de sécurité d'entreprises importantes où des infractions ont été perpétrées. Des mesures disciplinaires sont prises, l'employé a peut-être été mis à la porte, mais elles se contentent trop souvent de hausser les épaules ou décident simplement de ne pas tenter des poursuites judiciaires car elles savent que ces poursuites constitueront une perte d'énergie. Elles savent également que cela sera étalé dans la presse. C'est souvent le cas et personne n'aime admettre qu'il est vulnérable.

D'ailleurs, un de nos problèmes tient à ce que de nombreuses personnes pensent que si l'on parle des précautions que vous prenez, vous dites en fait aux gens comment les contourner, mais je ne suis pas d'accord. Je crois que de nombreuses sociétés ne parlent pas suffisamment des précautions qu'elles ont prises, ce qui en fait aurait pour conséquence de renforcer la confiance de leurs clients, de leurs employés et du public. C'est un problème de personnes et ces moyens de dissuasion dictent, dans une large mesure, le comportement adopté par le personnel et par les gens de l'extérieur.

Je suis sûr qu'un individu qui voudrait s'en prendre à une machine fixerait des priorités en fonction de la nature de la société. On connaît en général les sociétés qui sont gérées par des durs et celles qui sont vulnérables. C'est la même chose avec les boxeurs, je suppose. Cela devient une question d'émulation et rien de vous dissuade de ne pas le faire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'après ce que vous dites, j'ai l'impression que l'adoption d'une loi ou des modifications au Code criminel constitueraient en fait un moyen de dissuasion, mais je crois qu'il faut surtout s'attarder sur les amendes à imposer pour vols de données. Je ne sais pas quel critère guiderait la sentence à imposer dans des cas comme celui-ci. Je suppose, une fois de plus, que si un individu commet une infraction, si le vol de données constitue une infraction, il pourrait être emprisonné à perpétuité pour qu'il ne le refasse plus. C'est là une solution extrême, je suppose, mais comment en faire un moyen de dissuasion? Si la valeur que comporte le vol de données est extraordinaire, cela dépasse presque l'imagination si on en considère la valeur monétaire. Dans ce cas, rien ne décourage les gens de continuer à commettre des infractions, et vous avez utilisé tout à l'heure un exemple selon lequel le coupable est condamné à 60 jours pour avoir volé \$800,000 et ne passe que 40 jours en prison; mais en fait, s'il vole 250 millions ou milliards de dollars en utilisant les mêmes procédés et qu'il soit condamné à la prison à perpétuité, qu'en retirerait-il? Il réfléchirait d'abord aux chances qu'il a d'être pris en flagrant délit.

En tant qu'avocat, et je m'occupe parfois d'affaires pénales, je n'ai jamais rencontré de gens qui s'attendaient à être arrêtés

[Text]

they committed an offence, because if they did, they would never commit the offence in the first place, unless they were a complete fool.

• 1655

We used to get some rubby-dubs and winoes in the winter who used to wait till the policeman was driving past, then throw a bottle at a window and break it so they could go to jail and stay there for the winter. It would be nice and warm; they would get good food, and so on.

But really we are not talking about that kind of situation. How do you control it? I do not know that just passing a piece of legislation in itself, even with the kind of penalty provisions that might be provided, is actually going to do the job you want done. This really is what concerns me about it; the situation is going to remain the same.

But you did touch on something which concerns me greatly, and that is the ethics which you mentioned . . . the ethics in the business, the ethics of the people involved in working computers, and so on. It takes me back to university days. I remember when I was going into social work and was counselled in while some people were counselled out. Then when I went to law school, there was no counselling at all, either in or out. Maybe what you are talking about is that it needs this kind of preparation for people going into the business or into the field; that they should be sworn to some sort of secrecy; that they should take certain oaths, perhaps. I do not know what you are suggesting, but it means to me that it is such a sensitive area to get involved in that, if you are going to get involved in it at all, there needs to be not only some manual safeguard, but there has to be some kind of personal safeguard, so that the people who are getting into it are people of quality. It seems to me there are some questions which you might not be allowed to ask under the human rights legislation but which may properly have to be asked in this kind of situation.

Mr. Rous: We have a situation here basically where technology has run well ahead of society. There is no single approach. We need the educational system inculcating ethics; we need ourselves and the business community inculcating attitudes; we need the press doing the same thing; we need the support of the legislators saying this is condoned or not condoned.

It is a mass attack and we do not expect any one of these measures by itself to be effective; we do not expect a combination of them to be effective for a number of years yet. But I think those of us who are in a position to act—and that includes people like yourselves and ourselves and people like university educators—must start acting in concert with each other as opposed to acting in little bits and pieces here and there. Today we know of only one university course in Canada in computing science on the ethics of computing, and that is given at Western, I believe. It is a voluntary course and about 12 students a year sign up for it.

So far as we know, there is no other university which, in its computer science department, includes anything on ethics. We need their support as well. And if we were provided a forum

[Translation]

après avoir commis une infraction, car si cela avait été le cas, ils ne l'auraient jamais fait à moins d'être de parfaits crétins.

Évidemment, l'hiver, des ivrognes et des clochards attendaient qu'un agent de police passe pour jeter une bouteille dans une vitrine, la casser pour se faire mettre en prison et y rester tout l'hiver. Ils auraient été au chaud, auraient bien mangé, etc.

Mais là n'est pas la question. Comment contrôler cette situation? Je ne sais pas si la simple adoption d'un texte législatif, même comportant des amendes, réussira à juguler le problème. C'est ce qui me préoccupe le plus car je crains que la situation ne demeure la même.

Mais vous avez parlé quelques brefs instants de quelque chose qui m'inquiète beaucoup, je veux parler de l'éthique de la profession, la moralité de ceux qui s'occupent des ordinateurs etc. Cela me rappelle l'époque où j'étais étudiant à l'université. Je me souviens que lorsque j'envisageais de m'orienter vers le travail social, on m'avait fortement encouragé à le faire alors qu'on en avait dissuadé d'autres. J'ai ensuite décidé d'étudier le droit et là, personne ne nous a donné de conseils dans un sens ou dans l'autre. Or, dans le cas qui nous occupe, il faudrait peut-être faire subir ce genre de préparation à ceux qui s'orientent dans cette branche, ils devraient peut-être être assermentés d'une façon ou d'une autre. Je ne sais pas ce que vous suggérez, mais il me semble qu'il s'agit d'un domaine si délicat que non seulement des dispositifs de protection matérielle sont nécessaires mais qu'il doit y avoir également certaines garanties personnelles pour que ceux qui s'orientent dans cette branche soient fiables. Il me semble que la législation sur les droits de la personne vous empêche de poser certaines questions, qu'il y aurait justement lieu de poser dans ce cas.

M. Rous: En fait, nous sommes dans un monde où la technologie a quelques longueurs d'avance sur la société. Il n'y a pas une seule façon d'aborder le problème. Notre système éducatif devrait enseigner l'éthique, nous-mêmes et les entreprises devrions inculquer certaines attitudes, la presse devrait faire la même chose et nous avons besoin de l'appui des législateurs pour rendre illégales telles ou telles activités.

C'est un problème capital et nous ne nous attendons pas à ce qu'aucune de ces mesures soit en elle-même efficace, pas plus que nous ne nous attendons à ce que l'ensemble de ces mesures soient efficaces d'ici peu. Mais ceux d'entre nous qui peuvent agir, et je pense aux législateurs, à des gens comme nous ou aux professeurs d'université, devraient se mettre à agir en concert au lieu d'agir ici ou là par petits bouts. Il existe aujourd'hui un seul cours en sciences informatiques au Canada qui porte sur l'éthique de cette science et ce cours est donné à la *Western University*, je crois. Il s'agit d'un cours facultatif et seulement 12 étudiants s'y inscrivent par an.

Autant que nous sachions, il n'existe aucune autre université qui ne donne un cours sur l'éthique dans le cadre des sciences informatiques. Nous avons également besoin de l'appui des

[Texte]

like this in the educational community, we would be saying very much the same sort of thing but directing it towards them and their educational role, as opposed to towards you and your legislative role.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Could we then analogize to some extent with, say, the situation in most law schools? Certainly in Ontario, the law schools and the Law Society of Upper Canada have a code of ethics which you have to follow. It is not just business ethics; it is a code of personal ethics and professional ethics. They follow this very closely and very carefully. Should there not also be a body set up of people, although I do not know who they would be, but of people in the computer industry, who would monitor the industry itself, be responsible for it, set up codes of ethics and so on? Is this being done? Is it being contemplated?

Mr. Rous: It is being looked at.

Mr. Finch: I would like to comment on this. I will come back to ethics, but first of all, we realize that the Criminal Code is for the more severe violations of justice. We know that in some ways computer abuse is not consistent with the taking of life or some dastardly deed. At the same time, a computer crime, we also know, can contribute to very serious and extensive monetary losses. We know, too, because computers are used in all forms of control mechanisms in medicine and so forth, it could contribute to the loss of life itself.

So in those cases, when should someone purposely interfere with a computer program? In many cases we have not even discussed the aspect of robotics, where a machine kills a person.

• 1700

Mr. Rous: The first robot murder was . . .

Mr. Finch: You know this, I think, puts it on the same level of severity as other crimes that would come under the Criminal Code. I do recognize that it is very sensitive; certainly seemingly minor, or actually trivial violations should not be subject to a severe penalty. The problem is that once the person starts, we do not know where it will end, and we do not know the consequences.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): But you are not suggesting that the only safeguard should be in the Criminal Code provisions?

Mr. Finch: No, no, although I am registering a problem that we have experienced to date in civil law for the business man who does not have an army of lawyers at his disposal, the time, the dollars to expend, trying to bring to justice a person who, in his opinion, is a threat to business, as opposed to society. That is a problem, and I am sure there are a variety of ways of handling it.

[Traduction]

universités. Et si nous pouvions bénéficier d'une tribune comme celle-ci au sein de la communauté universitaire, nous leur dirions à peu près la même chose, mais nous insisterions sur le rôle éducatif tout comme nous insistons sur votre rôle législatif.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Peut-on alors établir une certaine analogie avec ce qui se passe dans la plupart des facultés de droit? En Ontario, les facultés de droit et la *Law Society of Upper Canada* possèdent un code de déontologie qu'il faut suivre. Il ne porte pas uniquement sur l'éthique de ce que vous pratiquez, mais également sur l'éthique personnelle et la déontologie professionnelle. Ceci est très important et ils sont très sévères à ce sujet. Ne devrait-on pas dans ce cas créer un organisme, bien que je ne sache pas qui en ferait partie, regroupant les industriels de l'informatique, qui seraient chargés de surveiller ce secteur, d'en être responsables, d'élaborer des codes de déontologie et ainsi de suite? Est-ce que vous envisagez de le faire?

M. Rous: On l'envisage effectivement.

M. Finch: Je voudrais faire une observation à ce sujet. Je reviendrai tout à l'heure sur cette question de déontologie, mais tout d'abord, permettez-moi de vous dire que nous sommes tous conscients que le Code criminel vise les infractions graves. Nous savons que, d'une certaine façon, le cambriolage informatique ne peut être comparé à un assassinat ou à un autre crime infame. Cependant, la piraterie informatique peut entraîner, comme nous le savons tous, d'importantes pertes monétaires. Nous savons également puisque des ordinateurs sont utilisés sur des machines médicales et ainsi de suite, que cela pourrait mettre en danger des vies humaines.

Alors, dans ces cas, à quel moment quelqu'un est-il considéré comme en train de violer sciemment un programme informatique? Dans de nombreux cas, nous n'avons même pas discuté de la robotique, lorsqu'une machine tue un individu.

M. Rous: Le premier meurtre perpétré par un robot a été . . .

M. Finch: Vous savez sans doute que la gravité dans ce cas est la même que pour tout autre crime relevant du Code criminel. Je reconnais que c'est un problème délicat; il est évident que des infractions mineures ou sans grande importance ne devraient pas faire l'objet de peines sévères. L'ennui c'est qu'une fois que la personne commence, nous ne savons pas où elle va s'arrêter et nous n'en connaissons pas les conséquences.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais cela ne veut pas dire que l'unique garantie devrait figurer dans le Code criminel?

M. Finch: Non, absolument pas, bien que je parle d'un problème qui se pose en droit civil pour l'homme d'affaires qui n'a pas une armée d'avocats à sa disposition, ni le temps et l'argent lui permettant d'intenter des poursuites judiciaires contre un individu, qui, à son avis, constitue une menace pour son entreprise plutôt que pour la société. C'est un problème qui se pose je suis sûr et qu'il y a 36 façons de le résoudre.

[Text]

On the ethics problem, I would like to suggest that there are deeper problems in the control of those people in the industry than we see with engineers, doctors and dentists; that is because the discipline is new, and because we are, at this stage in Canada at any event, unable to have the deterrent, for example, of taking away a person's licence to practice. We have run a very thin line, and I have been involved extensively over the past dozen years in discussions with the Canadian Information Processing Society on a code of ethics. As a matter of fact, most data processing organizations have a code of ethics, and most of us do abide by that code, which is a motherhood code that says we will honour our commitments to employers and so forth.

The problem is that people can practice without being members of those associations, and we are always walking on the thin edge between what is known in a computer system, and what is acceptable practice, and new systems which have never been tried before. Because the industry is moving ahead so quickly, each of us, every day, is faced with a new application of a computer in a way that we have never tried before. So we cannot be sure whether we are competent or not to do it.

Having said that, I would like to suggest that we are preaching to those people in church. We still have that great body of the public now that is not within the profession, if there is a profession.

Mr. Beatty: Those at the Dalton School were not licensed.

Mr. Finch: Yes. Or supposing it just happened to be not the Dalton School, but a group of 16-year-olds, or 66-year-olds, who had a computer terminal and decided to have a little fun. It is in that framework that a person feels free. We travel through the West Block Building here. We suddenly come across a computer terminal. We say, by golly, I wonder where that goes, and we notice, gee, it is still logged on. And we try and the first thing we know we have access to programs. And we say, gee, is that not interesting. I wonder what program this is, and so we look at it. There is no sense that says this is wrong; that this is immoral; you should not be doing this. You may be on, or close to a public corridor, but this is private property; keep out.

Now, there is a greater problem, as you pointed out, in the public areas. Certainly if someone sets up a Telidon system in a shopping centre, I believe that person is inviting all the public to abuse that system in any way they can—kick it, smash it, poke it, push it; you know, it is there. I think the same goes, to some extent, for the ATM machines of the banks. You are putting it in a public spot. You must have taken the precaution to make sure that this machine will not run amuck and will protect your business. It is this public feeling that this is new technology to be explored, and it is wonderful and let us explore it. I guess it is in that sense that we are appealing to start to have a basis. Many people do not believe that a thing is wrong unless there is a law against it,

[Translation]

Pour ce qui est de la déontologie, je crois que la déontologie qui s'applique aux industriels de l'informatique sont plus profonds que ceux qui s'appliquent aux ingénieurs, aux médecins et aux dentistes; c'est parce qu'il s'agit d'une discipline nouvelle et parce que nous ne pouvons pas, du moins pour le moment au Canada, retirer le permis d'exercer d'un individu. Le problème est délicat et je suis depuis une douzaine d'années en pourparlers avec l'Association canadienne de l'informatique à propos de l'établissement d'un code de déontologie. D'ailleurs, la plupart des organismes de traitement de l'information en possèdent un et la plupart d'entre nous le respectent dans le sens où nous promettons de respecter nos engagements pris envers nos employeurs et ainsi de suite.

Mais certains peuvent exercer leur métier sans être membre de ces Associations et nous sommes toujours à la frontière entre ce qui est connu dans un système informatique, ce qui est un usage acceptable, et des systèmes nouveaux qui n'ont jamais été testés auparavant. Ce secteur est si innovateur que chacun d'entre nous, chaque jour, est confronté à une nouvelle application d'un ordinateur, application qui n'a jamais été testée auparavant. Donc, nous ne savons jamais si nous pouvons bien le faire ou pas.

Cela dit, nous continuons à éduquer les gens, car il faut sensibiliser ceux qui ne font pas partie de la profession, si profession il y a, à la situation.

Mr. Beatty: Ceux qui fréquentaient la *Dalton School* ne possédaient pas de permis.

Mr. Finch: Effectivement. Mais supposons qu'il ne s'agissait pas de la *Dalton School*, mais d'un groupe de gens de 16 ans ou de 66 ans qui possédaient un terminal et avaient décidé de s'amuser. C'est dans ce contexte qu'une personne se sent libre. Par exemple, en se promenant dans l'Édifice de l'Ouest, on tombe soudain en arrêt devant un terminal. On se demande alors à quoi sert cet ordinateur jusqu'au moment où l'on remarque qu'il est en communication. On s'essaie à presser quelques touches et on constate que nous avons accès à certains programmes. Et on se dit que cela devient très intéressant. On se demande quel programme il s'agit et on le regarde. On ne pense pas que c'est illégal, immoral et qu'on ne devrait pas le faire. Vous pourriez vous trouver dans un corridor ou près d'un corridor, mais il s'agit en fait d'une propriété privée et vous ne devriez pas vous en approcher.

Mais il y a un problème plus grave qui se pose, comme vous l'avez dit, dans les endroits publics. Si quelqu'un installe un système Telidon dans un centre d'achats, je crois que cette personne invite en fait tout le public à faire ce qu'il veut avec ce système: lui donner des coups de pied, le casser, l'enfoncer, le pousser puisqu'il se trouve là. Dans une certaine mesure, cela vaut également pour les guichets automatiques des banques. Elles se trouvent dans un endroit public. Vous aurez dû auparavant prendre la précaution de vous assurer que cette machine ne se dérèglera pas et qu'elle protégera vos affaires. Le public pense qu'il s'agit d'une nouvelle machine, que c'est extraordinaire et il se sent presque obligé de la tripoter. C'est la raison pour laquelle nous voulons une base. De nombreuses personnes pensent qu'une chose est légale tant qu'il n'existe

[Texte]

and I guess the sum of it is that we would like to see a law against it.

• 1705

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): We are already past our time of adjournment, but if our witnesses are prepared to stay a bit longer . . .

Mr. Beatty: I just have a couple of brief questions, if you have time.

Mr. Finch: We are at your disposal.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I have several more questions, too, that I would like to put to you while we have you here.

Mr. Finch: I apologize for being long-winded.

Mr. Beatty: No, it is very helpful to us and I think the record will be very useful, as well, to other people studying the problem, because of your expertise.

Just going back to the chairman's point a minute ago, I think probably, first of all, the analogy to bank robbery, again, is useful in dealing with the chairman's concern. It does not matter what criminal penalty you attach to bank robbery, there will always be someone who is going to rob banks; but the fact is that the criminal penalty that is attached to it will deter a good number, a good percentage, of the people who otherwise would do it. The fact that you have made bank robbery a criminal offence does not, in any way, take away the responsibility of the banks themselves to make sure that their vaults are properly locked. But the fact that the vaults may not be properly locked does not deter from the fact that bank robbery is still a crime. It seems to me that the two are complementary.

Secondly, I think Mr. Finch put his figure on the key point. While it is very useful to encourage codes of ethics for people in the industry, and I think that is constructive, you cannot delicense a person who is not in a licensed profession. We are talking about a crime here that is extremely democratic; the knowledge that is necessary, and the technology that is necessary, to commit it are very widespread. There is no way in which any professional society could control it internally, through internal disciplinary measures in some way.

Could we go back to your proposals on how it should be dealt with, particularly with regard to unauthorized access? How would you deal with that on a time-sharing system, where I am a customer who has a right to get into the data bank and then I damage somebody else's material held in a computer to which I have authorized access?

Mr. Finch: I think, Mr. Beatty, Mr. Chairman, the person presumably, in this scenario, is an authorized user of the time-sharing system—in other words, he is allowed to be on it—and there are levels of protection. Colin Rous gave you a bit of the scenario of how you log on. The first one is: Who are you? I am Jim Finch. Are you entitled to use this system? Yes, I am.

[Traduction]

pas de loi la condamnant et, pour résumer la situation, nous aimerions qu'il y ait une loi condamnant ces pratiques.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Nous avons dépassé l'heure prévue pour la fin de nos travaux, mais si nos témoins sont prêts à rester encore un peu . . .

M. Beatty: Je n'ai que deux ou trois brèves questions.

M. Finch: Nous sommes à votre disposition.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'en ai encore plusieurs autres, quant à moi. Je voudrais profiter de l'occasion.

M. Finch: Je m'excuse d'être aussi long dans mes réponses.

M. Beatty: Vos connaissances nous sont d'un grand secours et intéresseront sûrement tout ceux qui se penchent sur la question.

Pour revenir à ce que disait le président tout à l'heure, l'analogie avec le vol de banque est utile. Elle illustre bien ce genre de préoccupations. Quelles que soient les peines prévues pour le vol de banque, il y aura toujours des vols de banque. Cependant, les peines prévues peuvent arriver à décourager un bon nombre de candidats au crime. Il reste que le fait de considérer le vol de banque comme une infraction criminelle ne diminue en rien la responsabilité des banques elles-mêmes de veiller à ce que leurs voûtes soient bien protégées. De toute façon, qu'elles soient bien ou mal protégées, le vol de banque reste une infraction criminelle. Les deux choses se complètent.

Par ailleurs, M. Finch a bien identifié le problème. Il pourrait être utile d'avancer des codes d'éthique pour les gens qui travaillent dans l'industrie, ce pourrait être une suggestion constructive, mais il est impossible d'enlever la reconnaissance professionnelle à quelqu'un qui ne se trouve pas dans une profession où il faut un permis pour travailler. Dans ce cas-ci, il s'agit d'un crime qui est à la portée de tout le monde; les connaissances et la technologie nécessaires sont le lot d'un grand nombre de personnes. Aucune société professionnelle ne parviendrait à contrôler l'industrie à partir de l'intérieur, au moyen de mesures disciplinaires internes.

Revenons aux solutions possibles, en particulier pour ce qui est de l'accès non autorisé. Lorsqu'il y a un partage du temps, que je suis client et que j'ai le droit d'accéder à la banque de données, si j'endommage la propriété de quelqu'un d'autre à l'intérieur du système, que peut-on faire?

M. Finch: Si la personne est autorisée à avoir accès au système, sur la base du temps partagé, il y a un certain niveau de protection. Colin Rous vous a donné un exemple de procédure d'entrée en communication. On vous demande d'abord: qui êtes-vous? Mon nom est Jim Finch. Avez-vous accès au système? Oui. Que voulez-vous faire? Je veux utiliser

[Text]

Then the question comes up: What do you want to do? I want to use this file. Am I entitled to use that file? Yes, I am. Let me have it.

Now the question comes up in relation to where I request the file that I am not authorized, or privileged, to have. I would maintain that, first of all, hopefully the system would not give me that file. However, it may be, through oversight, or just simple necessity because of the architecture of the system, that the system is not able to prevent me from taking that file. I would postulate that, at that point, I have trespassed across the line of honesty and am now embarking on a potentially wrong act. I have asked for something that is not mine. I could accidentally ask for something that I thought was mine and it turned out not to be, but the deeper I go in this instance the more—I do not want to use the word “criminal”, because of the intent of the Code—the more wrong my act becomes. Then it ranges from looking at information that I am not entitled to look at, taking information, or copying it, information that I should have no right to, and covering up my tracks so that nobody knew I was in there and looked at it.

Mr. Rous: The simple analogy there . . .

Mr. Beatty: So you would make those offences, as well as . . .

Mr. Finch: Yes, I would.

Mr. Rous: The simple analogy there is to look at the single company computer as being a private home and the time-sharing service bureau as being an apartment building. If I am the owner of one apartment in that building, that is the same as owning my house. If I accidentally—I am on the wrong floor . . . open the door and go into somebody else's apartment, that is one thing, but if I deliberately jimmy the lock and go into his apartment, that is exactly as if I had gone into his private house.

Mr. Beatty: Can we try another “for instance” here? Assume that we are on a public network. Let us say it is QL services, as a case in point, or some other system similar to that. What if I altered the data base and put false information on the data base or just changed something I did not particularly like in it?

• 1710

Mr. Rous: That is exactly why we were suggesting the focus should be on the activity. QL is a good example, because their data base is extremely large, and the users of it tend to trust the accuracy of the data. The fact that some data had been modified might never be discovered, and a lot of people might have acted upon false data, and therefore made wrong decisions, and therefore cost themselves a lot and might have done a lot of damage to themselves and to society in general; and it would never be known that somebody had committed the offence of modifying the data.

If the offence is unauthorized access to it, then that is much simpler to show. Now, we are not suggesting unauthorized modification should not be an offence. It is obviously a more severe offence, and I think the trend in most legislation is to

[Translation]

tel dossier. Êtes-vous autorisé à avoir accès à ce dossier? Oui. Mettez-moi en communication.

La question est de savoir si je pourrais avoir accès à un dossier pour lequel je n'ai pas d'autorisation. Je pense, d'abord, que le système ne me donnerait pas accès à ce dossier. Cependant, il se pourrait toujours qu'une erreur se produise ou que le système ait un défaut de construction quelconque et que j'y accède finalement. Dans ce cas, je saurais très bien que je dépasse les bornes de l'honnêteté et que je commets un acte répréhensible. Il s'agirait de quelque chose qui ne m'appartiendrait pas. Il se pourrait toujours que j'aie été amené là par erreur, mais plus je persisterais, plus mon acte deviendrait répréhensible, je ne veux pas utiliser le terme «criminel», à cause de l'intention qui est prévue dans le code. À partir de là, il y aurait toute une gamme d'infractions possibles. Je pourrais examiner des données que je ne suis pas autorisé à examiner, en tirer certains renseignements, les copier, cacher l'acte que j'ai commis de façon à ce que personne ne puisse s'apercevoir de ce que j'ai fait.

M. Rous: L'analogie la plus simple . . .

M. Beatty: Vous verriez là des infractions, tout comme . . .

M. Finch: Oui.

M. Rous: L'analogie la plus simple consiste à considérer l'ordinateur appartenant à une compagnie comme une maison privée et le bureau de partage du temps comme à un immeuble à appartements. Si je suis propriétaire d'un appartement dans un tel immeuble, c'est la même chose que si je possédais une maison. Si je me trouve au mauvais étage et que j'entre, par accident, dans l'appartement de quelqu'un d'autre, c'est une chose. Cependant, si je force la serrure de cet appartement, c'est la même chose que si je forçais l'entrée d'une maison privée.

M. Beatty: Prenons un autre exemple. Supposons que nous avons affaire à un réseau public. Prenons par exemple la Société *QL Systems* ou un système semblable. Qu'est-ce qui arriverait si j'introduisais de fausses données dans la base de données ou si je changeais simplement des données qui ne me plaisaient pas?

M. Rous: C'est précisément la raison pour laquelle nous avons dit qu'on devrait se concentrer sur l'activité en question. La *QL Systems* est un bon exemple, car sa base de données est extrêmement importante, et ses utilisateurs ont tendance à se fier aux données. Il est possible qu'on ne découvre jamais que quelqu'un a modifié les données. Dans un tel cas, beaucoup de personnes pourraient prendre des décisions qui seraient fondées sur de fausses données, et donc prendre les mauvaises décisions, ce qui leur coûtera très cher et pourrait faire beaucoup de mal à elles-mêmes et à la société en général.

Il est beaucoup plus facile de prouver l'infraction d'accès non autorisée aux données, que celle de modification non autorisée. Nous ne voulons pas dire par là que la modification non autorisée des données ne devrait pas être une infraction,

[Texte]

have a sliding scale of offences. What we are saying is the offence has to start with the unauthorized access in the first place.

Mr. Beatty: I think that is useful for me. I was concerned initially, when Mr. Finch mentioned unauthorized access, that he saw that as the entirety of the crime . . .

Mr. Rous: Certainly not.

Mr. Beatty: —or the potential offence.

It seems to me as well we might want to take a territorial approach. I am intrigued in physical security, to compare the security in these buildings, where once you make it past the guard at the front door you have free rein of the buildings. Compare that, with, for example, the State Department in Washington, where there is no guard at the front door. In each wing, they have security; and it is easy to get into the building, but you must demonstrate before you go into a wing that you have authorization to be there.

Mr. Rous: That is the coming trend in computer security as well.

Mr. Beatty: Okay, you are in; and you can go into some aisles, but you cannot go into some others.

Mr. Rous: That is right. But carrying that analogy a little further, looking at this building, it is a beautiful example. In the not-too-distant past, there has been a lot of publicity about strengthening security on the Hill, et cetera. We came in the Wellington Street door of the West Block, where there was a big sign saying: closed to the public. We signed in. We said: could you direct us to Room 208, please? They said: what committee is that? We gave them a name, and nobody checked it. We signed our names, and nobody checked that we were, in fact, who we said we were. It is just proof of the fact that the best of security precautions can break down.

Mr. Finch: I am an imposter.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I would not say that is necessarily the best of security. Obviously, you should have been asked for your identification and who you were going to see. There should have been a telephone call made and all the rest of it to the committee secretary or something of that nature, or you should have been asked to contact an individual.

If somebody wants to come into my office to see me, it is not sufficient that they just come in and say: I want to see Ken Robinson. The guard will phone the office to find out if this person is expected, who they are, and to get an authorization from somebody they know.

Mr. Finch: What we are dealing with is human errors and omissions here. If we recognize there will always be human errors and omissions—and this relates back to your discussions with the senior executive of whether or not he had a secure company—then the next onus is on us as citizens. Do we feel a

[Traduction]

puisque'il s'agit d'une infraction plus grave. En effet, je pense que la plupart des lois ont tendance à prévoir plusieurs infractions de gravité différentes. Nous disons simplement que la première infraction est celle de l'accès non autorisé.

M. Beatty: Votre réponse m'est utile. J'avais des inquiétudes au début lorsque M. Finch a parlé de l'accès non autorisé, car je croyais qu'il considérerait cela comme étant l'unique infraction.

M. Rous: Certainement pas.

M. Beatty: Ou l'infraction éventuelle.

Il me semble également qu'on devrait tenir compte de l'aspect de la sécurité. La sécurité varie beaucoup selon les édifices. Dans certains, on peut circuler où on veut une fois qu'on a passé le gardien à la porte principale. Mais il n'y a pas de gardien à la porte principale du Département d'État à Washington. Il est facile d'entrer dans l'édifice, mais avant de pouvoir pénétrer dans une aile donnée, il faut démontrer au gardien que vous êtes autorisé de le faire.

M. Rous: Cette tendance devient de plus en plus répandue dans le domaine de la sécurité des ordinateurs également.

M. Beatty: Disons qu'on réussit à entrer dans un édifice et qu'on a droit à circuler dans certains couloirs, et pas dans d'autres.

M. Rous: C'est cela. Prenez, par exemple, l'édifice où nous nous trouvons actuellement. Il n'y a pas très longtemps on a beaucoup entendu parler d'un renforcement de la sécurité sur la colline etc. Nous sommes entrés par la porte qui donne sur la rue Wellington de l'Edifice de l'ouest, où il y avait un grand panneau qui disait: interdit au public. Nous avons signé le registre et nous avons demandé où se trouvait la pièce 208. On nous a demandé de quel comité il s'agissait, nous leur avons donné un nom, et personne ne l'a vérifié. De plus, personne n'a vérifié l'authenticité de nos signatures. Si je vous dis cela, c'est pour vous prouver que même les meilleurs systèmes de sécurité peuvent avoir des lacunes.

M. Finch: Je suis un imposteur.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À mon avis, il ne s'agit pas forcément d'un des meilleurs systèmes de sécurité. Il est évident qu'on aurait dû vous demander de montrer une pièce d'identité et de dire qui vous alliez voir. On aurait dû téléphoner au greffier, par exemple, pour vérifier votre identité.

Si quelqu'un veut me voir à mon bureau, il ne suffit pas que la personne dise simplement qu'elle veut voir Ken Robinson. Le gardien téléphone au bureau pour savoir si nous attendons la personne en question, qui elle est, et pour obtenir une autorisation d'entrée.

M. Finch: Il s'agit d'erreurs humaines et d'omissions. Si nous reconnaissons qu'il y aura toujours des erreurs humaines et des omissions—et ceci rejoint ce que vous nous avez dit au sujet de vos discussions avec un cadre d'une société au sujet de la sécurité de son entreprise—c'est à nous en tant que citoyens

[Text]

responsibility when we walk in that door? It is putting the responsibility on the other party.

For example, if I knew I were subject to some unfortunate type of reprimand, I would make darned sure I signed in properly and that I made sure everybody knew I was coming and so forth.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Beatty brought up a point I would just like to follow up on.

Mr. Beatty: I want to get back to another point of order, when you are finished.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes. Initially, you were talking about computer theft. Now, this was theft in-house and theft outside. But my understanding was that, at that time, there was no such thing as being able to modify the program on the computer from outside, but only from inside. Is that so?

Mr. Rous: No, that should be the case; but it is not always the case, sometimes as a result of the omission of the owner of the computer system in not putting precautions in place. Sometimes the owner of the system has put the precautions in place; but through a lapse in the procedures, it is still possible. There are a number of systems and physically modified programs we know of through which we could dial in from home. We should not be able to do so, but we can.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So it can be done from outside as well.

Mr. Rous: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): That is a very dangerous thing, indeed, without doubt. I do not really know that the public knows this. I think they know there is computer theft, but I do not realize they know there can be this modification from outside. In some cases, for example, people on the road may want to log a purchase order with the main frame in the head office, and you have to have that ability in some instances.

• 1715

Mr. Rous: There is an interesting point raised there, Mr. Chairman. A few weeks ago I addressed a Mensa group out in Calgary. Those people are supposedly the top 2% in intelligence, et cetera. It was an extremely well informed group in terms of knowing the politics of—well, you name it; their knowledge was extremely wide-ranging. And when we started telling them things in the area of privacy, computer security, and so on, they did not have a clue in the world that any of these things were possible. So if they did not know, you are dead right: the man in the street, the owner of a lot of these companies, does not have a clue in the world. There is a drastic need for an educational process and we see legislation as being part of that educational process as well as being an actual deterrent.

Mr. Beatty: Mr. Robinson put his finger on a very key point earlier which perhaps you could elaborate for us, and that is something I keep running into when I talk to people in

[Translation]

d'agir en conséquence. De cette façon, on déplace la responsabilité sur la personne qui entre dans un édifice.

Par exemple, si je savais que je serais réprimandé, j'aurais fait beaucoup d'efforts pour tout faire comme il faut.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je voudrais donner suite à un point soulevé par M. Beatty.

M. Beatty: J'ai un autre rappel au Règlement lorsque vous aurez terminé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui. Au début, vous parliez de vol informatique qui se faisait et à l'intérieur et à l'extérieur d'une entreprise. Mais si je comprends bien, il est impossible que modifier le logiciel de l'extérieur, cela ne peut se faire que de l'intérieur. Ai-je raison?

M. Rous: Non, cela devrait toujours être le cas, mais parfois le propriétaire d'un système informatique ne prend pas suffisamment de précautions, ou parfois il y a simplement une lacune, cela arrive. À notre connaissance, il existe plusieurs systèmes et plusieurs programmes qui ont été modifiés et auxquels nous pourrions avoir accès par téléphone. Nous ne devrions pas pouvoir le faire, mais telle est la situation.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Donc cela peut se faire de l'extérieur également.

M. Rous: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il est indubitable que cela est très dangereux. Je me demande si le public est au courant de cela. Je pense que la population sait que le vol des données informatisées existe, mais je ne pense pas qu'elle sache que les programmes peuvent être modifiés de l'extérieur. Certains systèmes permettent, par exemple, à un employé qui voyage de consigner un ordre d'achat à l'ordinateur central du siège social.

M. Rous: C'est un point intéressant, monsieur le président. Il y a quelques semaines j'ai parlé à un groupe Mensa à Calgary. Les membres de ce groupe sont censés faire partie des 2 p. 100 les plus intelligents de la population. C'était un groupe bien informé dans toutes sortes de domaines. Mais lorsqu'on leur a parlé de la vie privée, de la sécurité des ordinateurs, etc., ils n'avaient pas la moindre idée que de telles choses étaient possibles. Donc vous avez tout à fait raison: si ces gens n'étaient pas au courant, le grand public, et les propriétaires de beaucoup de ces sociétés ne sont certainement pas au courant. Il existe un besoin urgent d'informer la population, et à notre avis une loi aiderait à cet égard et constituerait également un élément de dissuasion.

M. Beatty: M. Robinson a touché à un point clé tout à l'heure qui revient souvent lors de mes discussions avec les gens qui travaillent dans le secteur privé. Il s'agit de la probabilité

[Texte]

industry. That is the probability of being caught. One of your greatest deterrents is whether or not a perpetrator of an offence believes there is a possibility of his being caught. What sort of guidance can you give us as to what the probability is of detection for computer crime? Is it more likely to be detected than a physical crime of some sort, or is it less likely? Can companies build security that will make it easier for them to detect crime?

Even if a law is passed, is it a case where we will still only get the tip of the iceberg? In the vast percentage of cases the person is dealing with probabilities which are very good, but it may be far easier perhaps to rob an institution by computer than physically, if the risk that one takes, even with the law in place, is much less.

Mr. Finch: I would like to respond. It is possible; we are recommending it, and many companies are doing things that will allow them to detect. We have learned for the most part how to detect when something has gone wrong. We are in the process, I guess, of the state of our art in learning how to detect at a time when it is actually happening. But remember, in a computer several seconds is like a lifetime. It is not as obvious as a physical offence, of course, because there is no broken door, or you cannot walk into the room and obviously say, Look, something is ajar.

Again, we find problems, in that sometimes control procedures are in place, but computer staffs are notoriously understaffed; sometimes they do not take the time to check mechanisms that have been in place; the logging of transactions. For instance, we find many cases where people very fastidiously make sure that everyone who enters the computer room signs in, but often no one looks to see who actually did sign in that day.

So we can assure you that there is a great deal of progress from the technical point of view, in being able to discover that something has run amuck. It is difficult with text, as in QL, because you must understand the sense. But where there are control numbers, and unless the perpetrator has been very clever and perhaps has covered his tracks, generally there will be something funny and out of whack which will trigger an investigation into it.

Mr. Rous: But there is a difference between knowing that something happened and knowing who did it, if you only find it after the fact. The probabilities of getting caught today are infinitesimal; they really are extremely low.

Mr. Beatty: Is it technologically possible to cover your tracks entirely in getting into a computer system through a remote terminal site; copying data which, in the first place, you were not supposed to have access to in the system; second, there is confidential data in there that people did not want copied? Is it possible totally to cover your tracks or, given the time, would it be possible for you people to unravel the mystery and discover that an offence had taken place and obtain some idea of how it was committed? Can you completely erase any evidence of a crime having taken place?

[Traduction]

d'être découvert. L'un des principaux éléments de dissuasion est la possibilité d'être découvert. Que pouvez-vous nous dire au sujet de la probabilité de découvrir le coupable dans le cas des infractions relatives aux ordinateurs? Par rapport à d'autres infractions, est-il plus probable ou moins probable qu'une telle infraction sera découverte? Est-ce que les sociétés peuvent mettre sur pied des systèmes de sécurité qui faciliteront la découverte d'infractions?

Même si on adopte une loi, découvrira-t-on seulement un faible pourcentage des infractions dans ce domaine? Dans la plupart des cas, une personne qui commet une infraction court un grand risque d'être découverte. Il est peut-être beaucoup plus facile de voler par ordinateur plutôt que physiquement, car le risque qu'on court est beaucoup moindre, même avec l'adoption d'une loi.

M. Finch: Je voudrais répondre à la question. Il est possible de mettre en place des systèmes de sécurité, et c'est ce que nous recommandons à beaucoup de sociétés. En général, nous savons comment déceler s'il y a eu une «infraction» quelconque. Nous sommes en train d'apprendre comment déceler une action pendant qu'elle a lieu. Mais il faut se souvenir que dans le domaine des ordinateurs plusieurs secondes constituent une éternité. Ce genre d'infractions ne sont pas aussi évidentes que d'autres, car il n'y a pas de porte enfoncée, par exemple.

Parfois, même s'il existe des procédures de contrôle, le personnel est surchargé et ne prend pas le temps d'enregistrer toutes les opérations. Nous constatons que souvent on prend très soin de s'assurer que tout le monde qui entre dans la salle de l'ordinateur signe le registre, mais souvent personne ne vérifie qui a signé le registre.

Nous pouvons vous assurer qu'on a fait beaucoup de progrès du point de vue technique pour ce qui est du dépistage des problèmes. Dans le cas de la Q.L. Systems, il est difficile de déceler les problèmes, car on se sert d'un texte, et il faut comprendre le sens. Mais dans le cas de numéros de contrôle, à moins que l'auteur du crime ait été très astucieux et ait brouillé les pistes, en général il y a quelque chose qui cloche, et qui déclenche une enquête.

M. Rous: Mais même si on sait qu'il y a eu un crime, on n'en connaît pas toujours l'auteur, surtout si on n'est informé qu'après coup. A l'heure actuelle, la probabilité d'être découvert est extrêmement minime.

M. Beatty: Est-il possible du point de vue technique de brouiller les pistes tout à fait après avoir eu accès à un système informatique par l'intermédiaire d'un terminal à distance? Pourrait-on, de cette façon copier des données auxquelles on n'est pas censé avoir accès, des données qui sont peut-être confidentielles, et brouiller ensuite ses traces? Si vous aviez suffisamment de temps, vous serait-il possible de découvrir qu'il y a eu une infraction et comment elle fut commise? Est-il possible d'effacer tout à fait toute preuve d'un crime?

[Text]

Mr. Rous: In most cases that could be done, but it takes an extremely sophisticated person to do so.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Tell me, do you know if the computer manufacturers are working on something to safeguard?

• 1720

Mr. Rous: In 1972, IBM spent \$40 million on a computer security study. That is an awful lot of money. As a result of that, they did initiate some programs, and third-party people did. Honeywell has the system that resulted from the American project that I was talking about earlier. Some of the manufacturers are devoting a lot of resources to this.

However, stop and think about what their real interest is. Their interest is to sell computer systems to users. They do not want to frighten off that user by pointing out all of the potential dangers of using this system. So it is almost a conflict of interest. On the one hand, they recognize the responsibility to provide security; on the other hand, they recognize that it may be defeating their own sales force to point out to the users all of the potential dangers. So not as much is being done as could be done.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I see. What about Bell Telephone, Hydro, and others who have found ways of stopping the seeping away of the energy through lines, or whatever it may be? There must be some way that there can be detection of some sort. I suppose it is just a question of more technical development in the area to try to resolve this. Is there such a thing as having built into the computer a device that indicates when somebody is trying to take the information?

Mr. Rous: Yes, sir.

Mr. Finch: And these things are happening; but these things alone probably are not enough. We are still running behind; we are still in reactive mode.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I was talking to one company that indicated to me that they figured they had the safeguards already. What they do is they program the entry into the computer almost daily; the questions asked of it might be, for instance: My name is Ken Robinson, and the computer looks at it and says yes, you are one of the recognized people who can use the computer and the data; and then you are asked the question: are you authorized to use the data? and you say no. Maybe that is the answer that the computer wants—it is not a yes answer they want, they want a no answer. They were telling me that they foul it up or use different codes and so on to try to deter anybody who would be interested. But this was all done in-house.

Mr. Rous: Remember the first thing that I said: we do not know of any incidence of computer abuse on the record, with one exception, and that is the equity funding fraud, which is a weird case. But with that exception, we do not know of any of

[Translation]

M. Rous: Cela pourrait se faire dans la plupart des cas, mais il faudrait que l'auteur du crime ait des connaissances extrêmement avancées pour le faire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Savez-vous si les fabricants d'ordinateurs mettent au point un mécanisme de sécurité?

M. Rous: En 1972, IBM a dépensé 40 millions de dollars pour une étude sur la sécurité des ordinateurs. C'est une somme très considérable. Suite à cette étude, les responsables ont mis en place certains programmes, et d'autres l'ont fait également. Honeywell utilise le système qui a découlé du projet américain dont je parlais tout à l'heure. Certains des fabricants attribuent beaucoup de ressources à ce domaine.

Mais il faut se demander ce qui les intéresse véritablement. Avant tout, les fabricants veulent vendre des systèmes informatiques. Ils ne veulent pas donner peur à l'utilisateur en signalant tous les dangers éventuels du système. Il s'agit presque d'un conflit d'intérêts. D'un côté, ils reconnaissent la responsabilité de donner une certaine sécurité; mais d'un autre côté, ils savent qu'ils n'ont pas intérêt à signaler aux utilisateurs tous les dangers éventuels. Par conséquent, les fabricants ne font pas autant qu'ils pourraient faire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'accord. Qu'en est-il de Bell Canada, de l'Hydro et d'autres qui ont trouvé des moyens d'empêcher les crimes de ce genre? Il doit être possible de déceler ce genre de crime. Je suppose qu'il s'agit simplement d'avoir davantage de perfectionnements techniques afin de résoudre le problème. Peut-on intégrer à un ordinateur un appareil qui signale le fait que quelqu'un essaie de voler des données?

M. Rous: Oui, monsieur.

M. Finch: C'est le genre de progrès qu'on fait, mais cela ne suffit pas. Nous avons toujours du retard; nous sommes toujours en train de réagir après coup à des situations.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je parlais à des représentants d'une société qui m'ont dit qu'à leur avis ils ont déjà des mesures de sécurité. Ils changent presque quotidiennement le mot de passe nécessaire pour avoir accès à l'ordinateur. Par exemple, je pourrais dire à l'ordinateur que je m'appelle Ken Robinson, et l'ordinateur déciderait que je suis une des personnes qui est autorisé à utiliser l'ordinateur. Ensuite l'ordinateur me demanderait si je suis autorisé à utiliser les données et je répondrais que non. Il se peut que l'ordinateur soit programmé pour accueillir favorablement un non plutôt qu'un oui. Les responsables des sociétés m'expliquaient qu'ils utilisent des codes différents pour rendre l'accès à l'ordinateur plus difficile. Il s'agissait des mesures de sécurité internes.

M. Rous: Il ne faut pas oublier ce que j'ai dit au début: à l'exception du cas de fraude de capital, qui est un cas bizarre, nous ne connaissons pas de cas d'abus d'ordinateur qui n'auraient pas pu être empêchés si les sociétés avaient été au courant de la technologie actuelle.

[Texte]

them that could not have been prevented, given today's technology, had companies been aware enough to do that.

Now, another example of that—one of the Canadian banks introduced automated teller machines knowing that there was a significant risk that they would be stolen from. They did that for marketing reasons. It was a conscious decision to accept that risk, and sure enough they were stolen from through those automated teller machines. And they still said: okay, we lost x thousand dollars to the machines, but we gained x thousand dollars in keeping our customers and acquiring new customers; therefore it was worth our while.

There is always the question of how much money you are willing to spend to put these measures in place. There comes a point where it is no longer worth the money to go any further; therefore, you accept a certain amount of risk.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Would it be fair to say that the best advice you could give at the present time to anybody who has, say, very secretive information for their business or enterprise on a computer, would be to leave it out of the computer and put it in a safe?

Mr. Rous: That is absolutely the only advice, and we have made that recommendation to clients a number of times.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So basically what should be done is they should have a great deal of information that would not be too important, but the key elements should all be kept off that and merely put in as they need it.

Mr. Rous: Either that or kept on a separate computer system which does not have terminals all over the country and is not in a room available to people. There are a lot of secure installations. A room this size which contains one computer—there are no terminals outside this room, and this room is very heavily secured and we know exactly who is going in; the only things they can do when they are in there are things on that particular system. These things are all possible.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): There is just one other question I want to ask you and that is you made the statement that you did not feel that you wanted to get caught up in the trap of tying legislation to technology. I think this was the term you used. I am not just clear . . . you did talk about micro-magnetic, and this and that and the other thing, which is all too technical for me. Can you indicate to us, in a layman's terminology, what you mean by not tying the legislation to technology? Are we that far out of date, or out of step?

Mr. Rous: Well, yes. A good example: An awful lot of the American legislation refers to electronic devices. Right now in the laboratories there are experimental computers, which will be coming on the market in the next few years, that are optical, and biological is the next generation beyond that. If we define a computer as being an electronic device that does such and such, then as soon as I buy an optical computer the law no

[Traduction]

Permettez-moi de vous donner un autre exemple semblable. L'une des banques canadiennes a commencé à utiliser les caisses automatisées tout en sachant qu'il y avait un risque important de vol. Les responsables de la banque l'ont fait pour des raisons de commercialisation. Ils ont décidé d'accepter le risque, et il y a bel et bien eu des vols. La banque a décidé que même si elle avait perdu X milliers de dollars, elle en avait gagné davantage parce qu'elle gardait ses clients et en obtenait de nouveaux. Cela valait donc la peine.

Il y a toujours la question de savoir combien on veut dépenser pour mettre en place les mesures de sécurité. À un certain point, ce n'est plus rentable de dépenser davantage en mesures de sécurité; on décide simplement d'accepter un certain risque.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Est-il exact de dire que le meilleur conseil que vous pouvez donner à une société qui a des données très secrètes serait de les sortir de l'ordinateur et de les mettre dans un coffre-fort?

M. Rous: Tout à fait. C'est précisément ce que nous avons recommandé à plusieurs clients.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Autrement dit, les données les plus importantes ne devraient pas être introduites dans l'ordinateur avant qu'on en ait besoin.

M. Rous: On peut soit faire cela, soit avoir un autre système informatisé qui n'a pas de terminaux partout au pays et qui ne se trouve pas dans une salle d'ordinateurs accessible. Il y a beaucoup d'installations bien protégées. S'il n'y a qu'un ordinateur dans une salle, et s'il n'y a pas de terminaux en dehors de la salle, et si la salle est très bien protégée et qu'on sait exactement qui entre dans la salle, les possibilités d'abus sont limitées. Ce sont des choses qui peuvent être faites.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'ai une dernière question à vous poser. Vous avez dit qu'on ne devrait pas lier la loi à la technologie. Je pense que c'est ce que vous avez dit. Vous avez parlé d'appareils micro-magnétiques et de beaucoup de choses techniques qui me dépassent. Pouvez-vous nous expliquer en langage de profane ce que vous voulez dire lorsque vous dites qu'il ne faut pas lier la loi à la technologie? Sommes-nous si en retard sur la technologie?

M. Rous: Oui. En voici un bon exemple: beaucoup des lois américaines font allusion aux appareils électroniques. En ce moment, on est en train de faire des essais dans les laboratoires de certains ordinateurs optiques qui seront disponibles d'ici quelques années. Après les ordinateurs optiques, il y aura des ordinateurs biologiques. Si la loi définit un ordinateur comme étant un appareil électronique qui fait telle ou telle chose, un

[Text]

longer considers it a computer. That is a specific example of what it is that we are trying to avoid. As Jim said, if we had drawn up this legislation 25 years ago and we had defined it as being an electro-mechanical device, today none of these things would be computers, because we no longer have electro-mechanical devices as computers.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): What you are saying, then, is that the whole question of definition, today's definition, may be changed tomorrow.

Mr. Rous: That is right. Therefore, the definition should focus more on function than on technology.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): And that is what you meant when you said that the legislation should be tied into action, and not the definition itself.

Mr. Rous: That is correct.

Mr. Finch: Do not touch my information.

Mr. Rous: The definition should be as broad as possible, obviously while not including the whole world. The thing is that you want to keep out any kind of words that tie it to today's generation of computers.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I think we have pretty well exhausted your time and energy, and we certainly have lots to think about. It has been a very fruitful exchange, in my view. I am very pleased, indeed, that you could both appear before us. I would not be too sure but that we might not want to hear from you again, particularly, as we said at the beginning, if there may be something you could tell us in camera that would be helpful to us in dealing with our report, which will be forthcoming in the not too distant future. If you have any further suggestions to make at this time, I would be pleased if you would communicate with the Clerk of the Committee and let us know. We may want to get back to you again. Thank you very much for coming.

Mr. Finch: Thank you.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Just before we adjourn, the next meeting, I guess, will be at the call of the Chair. I think it will probably be next Tuesday at 3.30 p.m., in this same room.

The meeting is adjourned.

[Translation]

ordinateur optique n'est pas un ordinateur au sens de la loi. Voilà un exemple concret de la situation qu'il faut éviter. Comme Jim l'a dit, si on avait rédigé la loi il y a 25 ans et si on avait défini l'ordinateur comme étant un appareil électromécanique, aucun des appareils dont nous nous servons aujourd'hui ne serait un ordinateur au sens de la loi.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Autrement dit, la définition qu'on adopte aujourd'hui, pourra ne plus être valable demain.

M. Rous: C'est exact. La définition devrait donc viser davantage la fonction plutôt que la technologie de l'appareil.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Et c'est ce que vous voulez dire lorsque vous dites que la loi devrait viser des mesures concrètes.

M. Rous: C'est exact.

M. Finch: La loi doit prévoir qu'il ne faut pas toucher aux données d'autrui.

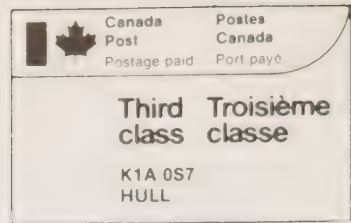
M. Rous: La définition devrait être aussi vaste que possible, sans être ridicule. Il faut éviter un libellé qui lie la définition à la génération actuelle d'ordinateurs.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il ne nous reste pas beaucoup de temps, mais vous nous avez certainement donné à réfléchir. La réunion a été très productive, à mon avis. Je suis certainement très content que vous ayez pu comparaître devant nous. Il se peut qu'on vous demande de comparaître de nouveau, surtout si vous pouviez nous dire quelque chose à huis clos qui nous serait utile pour la rédaction de notre rapport, qui devra se faire dans un avenir assez proche. Si vous avez d'autres propositions à nous faire, veuillez s'il vous plaît communiquer avec le greffier du Comité. Il se peut qu'on vous demande de comparaître de nouveau. Merci beaucoup d'être venus.

M. Finch: Merci.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): La prochaine séance aura lieu probablement mardi prochain à 15h30 dans la même salle.

La séance est levée.



If undelivered, return COVER ONLY to
Canadian Government Printing Office
Supply and Services Canada
45 Sacre-Coeur Boulevard
Hull, Quebec, Canada, K1A 0S7

En cas de non livraison
retourner cette COUVERTURE SEULEMENT à
Imprimerie du gouvernement canadien
Approvisionnement et Services Canada
45 boulevard Sacre Coeur
Hull, Quebec, Canada, K1A 0S7

WITNESSES—TÉMOINS

From Cerberus Computer Services Inc.:

Mr. James Finch, Toronto;
Mr. Collin C. Rous, Toronto.

De Cerberus Computer Services Inc.:

M. James Finch, Toronto;
M. Collin C. Rous, Toronto.

HOUSE OF COMMONS

Issue No. 3

Tuesday, April 19, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 3

Le mardi 19 avril 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

INCLUDING:

The First Report to the Standing Committee on Justice
and Legal Affairs

CONCERNANT:

Questions relatives à l'ordre de renvoi

Y COMPRIS:

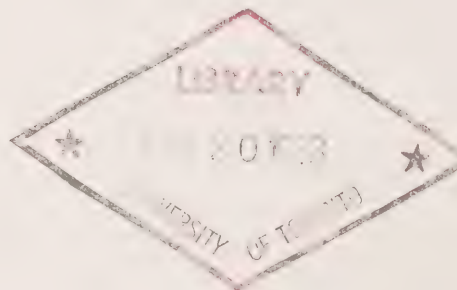
Le premier rapport au Comité permanent de la justice et
des questions juridiques

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS DÉSI-
GNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

**RAPPORT AU COMITÉ PERMANENT DE LA JUSTICE
ET DES QUESTIONS JURIDIQUES**

Le mardi 12 avril 1983

Le Sous-comité sur les infractions relatives aux ordinateurs
a l'honneur de présenter son

PREMIER RAPPORT

Conformément à son ordre de renvoi du mardi 1^{er} mars 1983, votre Sous-comité a commencé l'étude de l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs et demande la permission de poursuivre l'étude de son Ordre de renvoi après l'ajournement de Pâques.

**REPORT TO THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS**

Tuesday, April 12, 1983

The Sub-committee on computer crime has the honour to present its

FIRST REPORT

In accordance with the Order of Reference of Tuesday, March 1st, 1983, your Sub-committee has commenced consideration of the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime and requests leave to resume consideration of its Order of Reference after the Easter recess.

PROCÈS-VERBAL

LE MARDI 19 AVRIL 1983

(5)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h46, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membre substitut désigné présent: M. Robinson (Etobicoke—Lakeshore).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: De l'Association canadienne des fabricants d'équipement de bureau, Toronto: M. John Reid, président du Comité de législation (ACFEB), M. Howard Kaufman, vice-président de Xerox et M. John Dean, conseiller juridique sénior de IBM.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbaux du mardi 15 mars 1983, fascicule n° 1*).

Les témoins font des déclarations et répondent aux questions.

A 17h14, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation.

MINUTES OF PROCEEDINGS

TUESDAY, APRIL 19, 1983

(5)

[Text]

The Sub-committee on computer crime met this day at 3:36 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Céline Hervieux-Payette.

Designated Alternate Member present: Mr. Robinson (Etobicoke—Lakeshore).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From the Canadian Business Equipment Manufacturers Association, Toronto: Mr. John Reid, Chairman of the Legislation Committee (CBEMA), Mr. Howard Kaufman, Vice-President of Xerox and Mr. John Dean, Senior Legal Advisor of IBM.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings and Evidence, Tuesday, March 15, 1983, Issue No. 1*).

The witnesses made statements and answered questions.

At 5:14 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Tuesday, April 19, 1983

• 1543

Le président: La séance du Sous-comité sur les infractions relatives aux ordinateurs peut débuter.

Cet après-midi, nous avons le plaisir d'accueillir l'Association canadienne des fabricants d'équipement de bureau, représentée par MM. John Reid, Howard Kaufman et John Dean.

I would like to thank our experts for agreeing to appear before our committee. I welcome them for their help to this subcommittee of the Standing Committee on Justice and Legal Affairs in giving some recommendations to Parliament on the actual problem of computer crime.

Mr. John Reid (Chairman, Legislative Committee, Canadian Business Equipment Manufacturers Association): Thank you very much. My name is John Reid. I am chairman of the CBEMA legislative committee and legal counsel for Control Data Canada Ltd.

With me is Mr. John Dean, Senior Counsel, IBM Canada Ltd., and Mr. Howard Kaufman, Vice-President, Secretary and General Counsel with Xerox.

We are representing CBEMA today, which is the Canadian Business Equipment Manufacturers Association. It is composed of 69 member firms which manufacture and market a wide variety of business equipment in Canada, including word processors, copiers, typewriters, data processing equipment, as well as office and contract furniture. The revenues of our members exceeds \$6 billion and employ more than 50,000 Canadians.

• 1545

I would like to begin my remarks by extending a word of thanks to this committee for inviting us to appear this afternoon.

As you know, with the advent of the information society there has become greater and greater application of computers and computer services. Across a number of fronts it has become evident that regulations and legislation drafted in another era no longer suit the needs created by rapid developments in technology. This is certainly true with regard to computer-related crime.

The subcommittee has undertaken a very challenging task and we are pleased to be a part of your deliberations. I understand that copies of our presentation to the recent conference involving the Canadian Information Processing Society and the Department of Justice have been made

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mardi 19 avril 1983

The Chairman: I will call the meeting of the Sub-committee on computer crime to order.

Our witnesses this afternoon are Mr. John Reid, Mr. Howard Kaufman and Mr. John Dean from the Canadian Business Equipment Manufacturers Association. Welcome, gentlemen.

Je voudrais remercier nos experts d'avoir bien voulu comparaître aujourd'hui devant notre comité. Ils pourront aider ce sous-comité du Comité permanent de la justice et des questions juridiques à présenter certaines recommandations au Parlement sur le problème très réel que posent les délits informatiques.

M. John Reid (président, Comité législatif, Association canadienne des fabricants d'équipement de bureau): Merci beaucoup. Je m'appelle John Reid et je suis président du Comité législatif de l'Association canadienne des fabricants d'équipement de bureau ainsi que conseiller juridique pour la société *Control Data Canada Ltd.*

M'accompagnent, M. John Dean, conseil-expert pour IBM Canada et M. Howard Kaufman, vice-président, secrétaire et conseiller principal à Xerox Canada.

Nous représentons aujourd'hui l'ACFEB qui est l'Association canadienne des fabricants d'équipement de bureau. Notre association regroupe 69 sociétés membres qui fabriquent et commercialisent une vaste gamme d'équipement de bureau au Canada, notamment des machines de traitement de texte, des photocopieurs, des machines à écrire, du matériel de traitement des données, du matériel de bureau, et qui font de la location d'équipement de bureau. Les revenus de nos membres dépassent 6 milliards de dollars et ils emploient plus de 50,000 Canadiens.

Avant de commencer, permettez-moi de remercier ce comité de nous avoir invités à comparaître cet après-midi.

Comme vous le savez, l'avènement de l'ère de l'information a entraîné la multiplication des ordinateurs et des services d'information. Il est devenu évident que, dans certains secteurs, les règlements et les textes de loi adoptés antérieurement ne s'adaptent plus aux besoins créés par la révolution technologique. Cela est particulièrement vrai pour les délits informatiques.

Le sous-comité s'est attelé à une tâche très difficile et nous sommes heureux de participer à vos délibérations. Je crois que des copies de la présentation que nous avons faite lors d'une récente conférence à laquelle participaient la Société canadienne de l'informatique et le ministère de la Justice ont été

[Text]

available to the committee. If not, we have copies that we can leave with you.

Rather than repeat everything that is in the paper, I would like to highlight some of our major concerns and draw attention to the issues which I think would be of most interest to the members of this committee.

Mr. Robinson (Etobicoke—Lakeshore): Madam Chairman, on a point of order, I wonder if, since he is referring to a document, we could have a copy of it now.

Mr. J. Reid: Certainly.

Mr. Robinson (Etobicoke—Lakeshore): If you have any.

Mr. J. Reid: Yes, we do. How many would you like?

Mr. Robinson (Etobicoke—Lakeshore): Well, I would like one. I guess the other members would like one too.

Mr. J. Reid: After I have completed the overview, we would be pleased to answer any questions relating to the discussion paper or just on any matters generally.

You realize that data processing is a critical support system in business today. Because of its importance, the growth and scope of application, many risks are involved with the collection and retention of data. What we must also remember is that data is information; therefore, we are talking about privacy of information.

Information, at this point in time, is easily accessed whether intentionally or unintentionally by a wide number of users. An individual can gain access to data with virtual anonymity. Therefore, data theft or interference can be committed without obvious detection leaving victims in a difficult position.

First, they cannot detect whom, or why the theft or interference occurred; and secondly, they are unable to report it for fear of bad publicity and possible exposure to other incidents.

The lack of real legal measures to pursue, in order to obtain a conviction for data crimes, makes it even more unlikely that such crimes will be reported and perpetrators prosecuted. In our review of the present state of the law, as we have set out in our paper, we have touched on the inadequacies of the law as it exists today and discuss legislation required to remedy the situation.

If illicit computer activity is a concern to our society, we must realize that, because of the complexity of this issue, there is no one solution—in fact, several solutions should be considered. We feel that serious penalties are necessary when dealing with data abuse, as in other theft and abuse cases. Because current laws do not protect data, CBEMA would like

[Translation]

distribuées au comité. Dans le cas contraire, nous pouvons vous en laisser quelques-unes.

Au lieu de répéter tout ce que renferme notre document, je voudrais m'attarder sur certaines de nos principales préoccupations et attirer votre attention sur des questions qui, à mon avis, intéresseront particulièrement les membres de ce comité.

M. Robinson (Etobicoke—Lakeshore): Madame le président, un rappel au règlement. Je me demande si nous ne pourrions pas obtenir une copie maintenant du document auquel il fait allusion.

M. J. Reid: Mais absolument.

M. Robinson (Etobicoke—Lakeshore): Si vous en avez.

M. J. Reid: Oui, nous en avons. Combien en voulez-vous?

M. Robinson (Etobicoke—Lakeshore): Bien, j'en voudrais un exemplaire. Et je suppose que les autres membres du Comité en voudraient également un.

M. J. Reid: Après vous avoir donné un aperçu général de la situation, c'est avec plaisir que nous répondrons aux questions que vous voudrez bien poser à propos de notre mémoire ou à toute question générale.

Vous savez sans doute que le traitement des données constitue un moyen de soutien très critique dans le monde des affaires aujourd'hui. En raison de son importance, de la multiplication de ses applications et de la portée de celles-ci, la collecte et la conservation des données comportent de nombreux risques. Nous devons également garder à l'esprit que les données constituent en fait de l'information et que, par conséquent, nous parlons du caractère privé de cette information.

Un vaste nombre d'utilisateurs peuvent, à l'heure actuelle, accéder facilement à cette information, soit délibérément soit accidentellement. Tout individu peut avoir accès à des données dans l'anonymité presque complète. Par conséquent, le vol de données ou toute intrusion peuvent avoir lieu sans que cela se remarque immédiatement, laissant ainsi les victimes dans une position difficile.

Premièrement, celles-ci ne peuvent savoir qui est en cause ni pourquoi il y a eu vol ou intrusion. Deuxièmement, elles ne peuvent pas le faire savoir, craignant une mauvaise publicité et le renouvellement d'autres incidents.

L'absence de réelles mesures juridiques permettant d'intenter des poursuites judiciaires en vue d'obtenir des condamnations pour délit informatique rend encore plus difficile la notification de ces délits ainsi que la poursuite des auteurs de ces délits. L'examen de la loi, telle qu'elle se présente aujourd'hui, montre que cette loi présente certaines lacunes et, dans notre mémoire, nous proposons certaines mesures législatives qui s'imposent dans le but de redresser la situation.

Dans le domaine informatique, si toute activité illicite préoccupe tant notre société, c'est parce qu'il n'existe aucune solution unique et ce, en raison de la complexité du sujet. En fait, plusieurs solutions devraient être étudiées. Nous estimons que des peines sévères devraient être imposées pour délit informatique, comme pour toutes les affaires de vol ou autre

[Texte]

to see a separate section added to the Criminal Code that protects this private data and computer facilities from unauthorized use or access.

While we are talking today of computer abuse, we would like to point out, as we did in our brief, that the problem is much broader. What we are really dealing with is the protection of information regardless of form. We have suggested a solution of one aspect of what is a very large problem. We believe it is a problem that must be taken one step at a time, and this is the first step.

We, as an association, are prepared to assist the committee in continued revision and comments on any legislation that may result from your deliberations.

Now, we are prepared, if the committee wishes, to go through our paper section by section, giving general comments or just answer questions—whatever the committee wishes.

The Chairman: Mr. Robinson, what is your feeling? Would you like them to comment on it?

Mr. Robinson (Etobicoke—Lakeshore): I think it might be helpful if you commented on each page of your paper.

• 1550

Mr. J. Reid: Okay, I will. I will begin today. Basically our position is that today we are really in the information age and our ability to collect, process, analyse and retrieve information has made information a vital part of our economy. As we point out in the paper, services as opposed to products continue to grow in importance as a major portion of the gross national product. One of the problems is that information is an intangible, that knowledge, concepts, ideas, all of which comprise information, are abstractions. The value of this information is not the piece of information by itself. It really comes from the use that can be made of that information. After one has acquired information, one must protect it, because of its value, as we have said, which comes from what can be done with it or what you can prohibit somebody else from doing with it. Until recently the protection of data was really aimed at protecting the medium that the data was on, so we worried about file cabinets and vaults, and whatnot. We were really emphasizing, I guess, the physical manifestation but in today's environment technology has by-passed this. Today, with computers and the electronic age, we are in the situation where information can be stolen, can be altered, erased, modified, analysed, all without the owners' knowledge or authorization. The computer allows us to access information or to deal with information in a manner which really falls outside the laws as they exist today.

In the brief we set out four examples. I guess they are commonly referred to as computer abuse or computer crime. The first one is where you have a service bureau or data centre customer who is given a pass to enter into—this is on page 4 of the paper—where someone is authorized to get into the system but once he is in there just by random keyboarding can access

[Traduction]

abus. Puisque les lois actuelles ne protègent pas l'information, l'ACFEB propose qu'un article soit ajouté au Code criminel dans le but de protéger ces données privées et ces installations informatiques contre toute utilisation ou accès indus.

Puisque nous parlons aujourd'hui de délit informatique, nous aimerions faire remarquer, tout comme nous l'avons fait dans notre mémoire, que le problème est beaucoup plus vaste. Nous avons à faire face en fait à la protection de l'information quelle que soit la forme qu'elle revête. Nous avons proposé une solution à un aspect du problème qui est très vaste. Le problème doit être examiné étape par étape, et cette solution en constitue la première.

En tant qu'association, nous sommes tout à fait disposés à revoir et à commenter tout texte législatif qui ressortirait de vos délibérations.

Si le Comité le désire, nous sommes maintenant prêts à parcourir notre mémoire chapitre par chapitre, à en faire une analyse générale ou simplement à répondre à vos questions.

Le président: Monsieur Robinson, qu'en pensez-vous? Voudriez-vous qu'ils le commentent?

M. Robinson (Etobicoke—Lakeshore): Je crois que ce serait plus utile si vous commentiez chaque page de votre mémoire.

M. J. Reid: Très bien. C'est moi qui vais commencer. Fondamentalement, nous pensons que nous sommes entrés dans l'ère de l'information et que la possibilité que nous avons de rassembler, de traiter, d'analyser et de récupérer les données a fait de l'information une part importante de notre économie. Comme nous le faisons remarquer dans notre mémoire, les services par rapport aux produits constituent de plus en plus une part importante du produit national brut. Or, l'information est intangible, la connaissance, les concepts et les idées, c'est-à-dire l'information, sont des réalité abstraites. Cette information n'a aucune valeur intrinsèque. Tout dépend en réalité de l'utilisation qui en est faite. Une fois l'information emmagasinée, il faut la protéger, en raison de sa valeur, qui, comme nous l'avons dit, provient de ce qui peut en être fait ou de ce que vous pouvez faire pour empêcher quelqu'un de l'utiliser. Jusqu'à une date récente, les données étaient protégées en protégeant le support renfermant les données et nous nous préoccupions donc de classeurs, de coffres-forts et ainsi de suite. Nous mettons l'accent, je suppose, sur le support matériel, mais la révolution technologique actuelle a tout changé. De nos jours, avec l'avènement de l'ère informatique électronique, l'information peut être volée, modifiée, effacée, changée, analysée et ce, sans que les propriétaires le sachent ou l'autorisent. L'ordinateur nous permet d'avoir accès à l'information ou de la traiter sans que cet accès ou que ce traitement ne puisse être réglementé par les lois actuelles.

Nous citons quatre exemples dans notre mémoire. Cela s'appelle, dans le langage courant, des délits informatiques ou du piratage électronique. Voici un premier exemple: un client d'un bureau de services ou d'un centre de données se voit assigner un mot de passe, et ceci se trouve à la page 4 de notre mémoire, qui lui permet d'utiliser l'ordinateur, mais il peut

[Text]

another customer's data bank. Really he is an authorized user but he is then conducting unauthorized activity. One of the problems being that he can accidentally, if not wilfully, destroy or alter a part of someone else's data.

Then of course we have the example that I think has been in the paper from time to time, young... most of the time I guess it is a young computer enthusiast who for the sake of what we would call kicks, decides he is going to try and access the computer system and manages to get into somebody's data bank. The problem again is that while in there as a lark, if he does not know what he is doing, he can cause a great deal of damage.

We also point out the example of someone who is perhaps a bit disgruntled, and in writing a program decides to put in a command that if he is dismissed the program will self-erase. He is dismissed, the program goes, the company, or whoever, can be out a great deal of money, time and effort.

Also as a rather simple example of someone in a data processing division interested in obtaining a list of employees' addresses, phone numbers, or customers, or whatever, who during normal working hours commands a printout, gets all the information and proceeds to tuck it under his arm and walks out with it.

These are examples that we point out of various aspects, the different nature that the crime or abuse can take, and various areas we feel have to be dealt with.

I would now like to turn it over to Mr. Dean.

Mr. John Dean (Canadian Business Equipment Manufacturers Association): I would like to deal with the status of the law as it currently exists. Traditionally, the law dealt with the protection of things and people. However, information is neither a thing nor people; it is intangible, as John has said.

• 1555

The only laws that currently give protection for information are in the area of trademarks, copyright and patents, but these laws are somewhat limited in their ability to protect information. A copyright requires some form of copying; and it has a time limit, a life for the copyright. Patents require some degree of innovation associated with the knowledge or the information, and it also has a time limit. Trade marks deal with a very narrow part of the information spectrum.

The Criminal Code focuses only on things and people. Crimes involving fraud, mischief, theft or forgery all require some form of prohibited activity involving something tangible. As information has value, we feel it deserves protection, just as people and things are protected by the law. We, therefore, require some legislative enactment to provide complete, or more complete, protection for information.

[Translation]

très bien, en se servant au hasard du clavier, accéder à la banque de données d'un autre client. En fait, il est autorisé à utiliser l'ordinateur mais ce qu'il fait ne l'est pas. Or, un des problèmes qui se pose, c'est qu'il peut accidentellement, sinon volontairement, détruire ou modifier une partie des données d'un autre client.

Voici un deuxième exemple: on le retrouve parfois dans les journaux; il s'agit de jeunes amateurs d'ordinateurs, qui, par amusement, décident d'essayer d'avoir accès à l'ordinateur et c'est ainsi qu'ils réussissent à obtenir la banque de données d'un tiers. Là encore, alors qu'il s'amuse dans l'ordinateur, il peut faire beaucoup de tort s'il ne sait pas ce qu'il fait.

Comme troisième exemple, on pourrait citer un individu mécontent qui, en rédigeant un programme, décide d'y introduire une commande selon laquelle le programme s'auto-effacera s'il est licencié. Il est licencié, le programme est effacé et la société ou l'individu en cause peut essuyer de lourdes pertes financières, perdre beaucoup de temps et voir réduits à néant ses efforts.

Quatrième exemple: un employé du service de traitement des données qui voudrait obtenir une liste complète avec adresses et numéros de téléphone des employés ou des clients pourrait très bien, pendant ses heures normales de travail, imprimer cette liste puis partir avec celle-ci sous le bras.

Voilà donc des exemples qui témoignent du caractère fort divers que peuvent revêtir les délits informatiques et des domaines qui, à notre avis, devront être réglementés.

Je voudrais maintenant passer la parole à M. Dean.

M. John Dean (Association canadienne des fabricants d'équipement de bureau): Je voudrais parler de la loi actuelle et de ses applications. La loi a été de tout temps axée sur la protection des biens et des personnes. Cependant, l'information n'est ni un bien ni un individu, elle est de nature intangible, comme l'a dit John.

Seules les lois concernant les marques de commerce, les droits d'auteurs et les brevets d'invention assurent une certaine protection à l'information, mais ces lois sont quelque peu limitées. Pour enfreindre des droits d'auteurs, il faut procéder à une certaine forme de reproduction et ces droits d'auteurs ne sont pas protégés *ad vitam aeternam*. Les brevets d'invention exigent une certaine forme d'innovation liée à la connaissance ou à l'information et ceux-ci sont également limités dans le temps. Les marques de commerce sont très limitées dans le champ de l'information.

Le Code criminel ne se préoccupe que de biens et d'individus. Les délits, tels que la fraude, la malversation, le vol ou la contrefaçon, entraînent tous une forme d'activités interdites de nature tangible. L'information possède une certaine valeur et nous estimons qu'elle doit être protégée par la loi, tout comme les biens et les individus. Par conséquent, des mesures législatives devraient être adoptées pour permettre à l'information

[Texte]

One approach suggests amending the Criminal Code to broaden the definition of property to include information. As attractive an approach as it seems, it does come to grip with the subject of information, quite distinct and apart from computers, which are difficult to define from a legislative point of view; and that is the pro with respect to dealing with this subject by way of broadening the definition of property.

However, the con is that this approach would give certain characteristics traditionally reserved to tangibles, certain characteristics that the term "property" currently has that are reserved for tangibles, characteristics such as the exclusive right to use and dispose of the property.

Property carries with it some form of ownership that gives this exclusive right. Without changing the civil law, which is a provincial responsibility, such an approach would result in information being treated differently under the Criminal Code than under the civil law in areas such as trespass. Do not rush into an approach that expands the definition of the word "property" without addressing the civil law side of the issue. It would seem odd to punish a person for stealing data under the Criminal Code, when the victim cannot enforce property rights to recover damages from the accused who has taken the information.

I am going to now turn it over to Howard who will deal with some other approaches to solving this problem with respect to legislative enactment.

Mr. Howard Krofman (Canadian Business Equipment Manufacturers Association): What I will cover is found on pages 8 through 12 in our brief. I will be dealing with information and its use in the broadest sense. I will also touch on some of the ideas with respect to penalties that might be imposed in the event of unauthorized use of information.

The concept of information is not new to society. What is really new, as a result of computers, is the medium on which it is stored and manipulated, and its accessibility electronically. Information is only protected to a certain degree under the current law; but what a computer has done is point out the gaps the law has in protecting information in the general sense, which has been alluded to by Mr. Dean and Mr. Reid.

Some suggestions have been made that there is a need to protect information in its largest sense as opposed to a narrow sense, with only certain limited exceptions which could be precisely defined. In other words, where there is a will by someone on an organization to inform of or know about information, one could then limit the information to those who only need to know. So if there is no need, the acquisition of that information could be or should be prohibited from being accessed without consent, the idea being that only authorized used of that information would be allowed. If there is no authorization, an offence of some sort, be it criminal or civil, would then occur and consequent penalties would flow. Consent to the use of that information would be the prerogative of the holder of the information, rather than the owner.

[Traduction]

d'être protégée intégralement ou du moins de manière plus complète.

Certains proposent que le Code criminel soit modifié dans le but d'élargir la définition de «biens» pour y inclure l'information. Cette suggestion semble séduisante et permet de résoudre le problème que pose l'information, sujet fort différent de l'ordinateur, difficile à définir d'un point de vue législatif; voilà donc un des avantages qu'on en retirerait si la définition de «biens» était élargie.

Cependant, l'inconvénient qu'entraîne cette suggestion, c'est que certains traits caractéristiques réservés de tout temps aux réalités tangibles s'appliqueraient, je veux parler de certaines caractéristiques que revêt le terme «biens» comme le droit de jouissance et de cession exclusif du bien.

Dans le terme «biens», existe une notion de propriété qui lui donne ce droit exclusif. Sans modifier le droit civil, qui relève des provinces, cette suggestion permettrait de traiter l'information différemment dans le Code criminel plutôt que dans le droit civil dans des domaines tels que l'intrusion. Ne vous précipitez pas à modifier la définition du vocable «biens» sans vous pencher sur les conséquences que cela entraînerait en droit civil. Ce serait très bizarre de punir quelqu'un pour avoir volé des données en vertu du Code criminel, alors que la victime ne peut pas faire respecter ses droits de propriété en vue de récupérer des dommages et intérêts de celui qui a volé l'information.

Je vais maintenant céder la parole à Howard qui va proposer d'autres moyens de résoudre ce problème par voie législative.

M. Howard Krofman (Association canadienne des fabricants d'équipement de bureau): Ce dont je vais parler se trouve aux pages 8 à 13 de notre mémoire. Il s'agit de l'information et de ses utilisations diverses. Je parlerai également des peines qui pourraient être imposées en cas d'utilisation indue de l'information.

Le concept d'information n'en est pas un nouveau pour la société en général. Ce qui l'est, c'est le support dans lequel elle est stockée et manipulée et son accès par voie électronique. L'information n'est que peu protégée par la loi actuelle. Mais l'ordinateur a permis de montrer du doigt les lacunes que présente la loi lorsqu'il s'agit de protéger l'information au sens général, comme l'ont déjà dit M. Dean et M. Reid.

Certains disent qu'il faut protéger l'information dans son sens le plus large, sous réserve d'exceptions limitées définies par la loi. En d'autres termes, lorsqu'un employé d'une organisation désire avoir accès à certaines données, cet accès ne pourrait être donné qu'à ceux qui doivent y avoir accès. Si cette nécessité ne se présente pas, l'accès à cette information devrait alors être interdit sans autorisation, seule l'utilisation autorisée de cette information étant permise. En l'absence d'autorisation, une infraction, qu'elle soit criminelle ou civile, serait perpétrée et des sanctions s'imposeraient. Il reviendrait au détenteur de l'information et non pas au propriétaire de cette information de consentir à son utilisation car il est parfois très difficile de déterminer qui en est le propriétaire ou qui l'est

[Text]

This is mainly because of the difficulty, sometimes, in identifying who the owner might be, or determining who it might be at some point in time. There is always a holder of information, which is more easily defined.

• 1600

In this entire area one could go further and require that injury be present before an offence is complete. In other words, mere unauthorized use is not enough, but some economic or other injury must be suffered for the offence to have occurred.

This approach captures information in all its forms, not just electronic media and computerized information, but this suggestion does have its problems because there would be limitations on the enforceability of this kind of approach. Simple possession, or knowledge, without authority would not be an offence. The essence of the offence would be the use without authority and, of course, how proof of that unauthorized use is made is another difficult question, which this type of approach does not suggest. I mention it merely because there is that kind of thing, that one should look at where it finally leads. CBEMA yet has not determined in its own mind where that leads but it is something for consideration.

Another issue that relates to information is use of computer time and the services on a computer. Users of computers may have unused time on their own equipment, which they may wish to sell, and it is a form of reduction of cost when they do that. Equally, you have service bureaus whose only, or sole, or main function is to sell time on their computer, either the hardware or the programs they have put into place. In both cases, unauthorized users could enter into the computer to make use of the facility without payment.

Some may say, so what? What have you lost? You have not really lost anything, you were not going to earn anything anyway at that point in time. In our view, aside from the loss of revenue aspect—revenue should have been paid—there is the concept of unauthorized entry to something that is private. Perhaps an analogy is appropriate: If someone enters your house when you are away, is it not offensive, not to mention an offence, when that occurs? Why should entry into a computer system be any different? I may not rent my house out for revenue, but the fact that I am not doing it does not mean that somebody has a right to come in. The analogy is not totally complete, but the principle, I think, underlying it is something we are driving at—to be sure that the committee, in its deliberations, considers it seriously in that sense.

The difficulty with the current law is that it is not adequate to cover the unauthorized use of the computer. The McLaughlin case, which we referred to in our brief, at page 10, shows that attempts to prosecute this kind of activity under the current legislation, which is the unauthorized use of a telecommunications facility, is doomed, because essentially a computer

[Translation]

à un moment donné. Or, il est plus facile de définir qui détient l'information.

Dans ce domaine, on pourrait aller plus loin et statuer qu'il devrait y avoir tort avant qu'il y ait vraiment infraction. En d'autres termes, une utilisation indue de l'information ne suffirait pas, mais il faudrait qu'il y ait eu tort économique ou autre pour qu'une infraction soit considérée comme ayant été perpétrée.

Cette démarche permet de capter l'information sous toutes ses formes, non pas seulement les media électroniques et les données informatiques, mais cette suggestion pose cependant certains problèmes car il serait difficile de l'imposer. La simple possession d'information ou la simple connaissance de cette information sans autorisation ne constitueraient pas une infraction. Ce qui serait une infraction, serait de l'utiliser sans autorisation et nous sommes évidemment conscients du fait qu'il serait difficile de prouver que l'information en question a été utilisée de façon indue, ce que cette démarche ne mentionne pas. Je ne vous en fais part que parce que cela existe et parce qu'il faudrait en étudier les conséquences. L'ACFEB n'a pas encore pris position là-dessus, mais c'est une question à l'étude.

Un autre problème qui se pose est l'utilisation du temps-machine et des services informatiques. Les usagers peuvent très bien ne pas utiliser tout leur temps-machine et vouloir le vendre, ce qui permet de réduire les coûts. D'ailleurs, il existe des bureaux de services dont la fonction principale ou unique est de vendre du temps-machine, qu'il s'agisse de l'ordinateur lui-même ou des programmes qu'ils y ont introduits. Dans les deux cas, les usagers non autorisés pourraient avoir accès à l'ordinateur sans payer.

Certains vous diront: «Et alors? Qu'avez-vous perdu? Vous n'avez rien perdu en réalité car de toute façon vous n'alliez rien gagner.» À notre avis, mise à part la question de la perte de revenu, car nous estimons que le temps-machine devrait être rémunéré, se pose le problème de l'accès sans autorisation à quelque chose de privé. Une analogie s'impose peut-être: si quelqu'un s'introduit dans votre maison lorsque vous n'y êtes pas, n'y a-t-il pas infraction? Pourquoi cela ne vaudrait-il pas pour quelqu'un qui s'introduirait dans un système informatique? Il se peut très bien que je ne loue pas ma maison pour en tirer un revenu, mais ce n'est pas parce que je ne la loue pas que quelqu'un a le droit d'y entrer. L'analogie ne s'applique pas totalement mais le principe qui la sous-tend est ce que nous recherchons et nous voulons nous assurer que le Comité le verra également de cet oeil et étudiera la question sérieusement.

Or, il ne suffit pas de couvrir, par voie législative, l'utilisation non autorisée d'un ordinateur. L'affaire McLaughlin, dont nous parlons dans notre mémoire à la page 10, montre qu'il est inutile d'essayer d'intenter des poursuites judiciaires pour ce genre d'activités en vertu de la loi actuelle, qui couvre uniquement l'utilisation non autorisée d'un service de télécommunica-

[Texte]

facility has rightly, in our view, been determined not to be a telecommunications facility. The two are not the same.

The suggestion is that you need a separate and distinct section, if it is to be a criminal offence, that deals with computer facilities. This is a traditional solution to a problem, because what you are doing is capturing a particular item in a point of time. The computer industry has been known for its rapid technological development. This would, therefore, entail definitions that Parliament would have to consider on a regular basis to keep up with these technological developments, or else the law would be outstripped over a point in time.

Another aspect that needs to be considered, in our view, is the question of penalties, which relates directly to the concept of what is the value of the information that is being protected, or what is lost as a result of use, or misuse, abuse or theft. Information, in and of itself, probably has little value. It does not do anything for anybody. It is only when, in fact, it is being used that it has value. In other words, if it is put to use for someone's advantage, or to somebody's disadvantage, such that you have the benefit and the problem of a disadvantage, as the case may be, if you are to protect that kind of concept there has to be a penalty that would deter people from misusing information. In other words, the greater the injury or disadvantage to the victim, and the greater the gain or the advantage to the offender, in our view the greater the penalty. This will enable to establish a deterrent factor as well as punishment for the event of itself.

• 1605

We, therefore, feel that it is more appropriate in this circumstance to cover the basic theft of, or misuse or abuse of, computer facility time and information on a computer in the criminal side, with some requirement to be done on the civil side which, presumably, the provinces will address after or before whatever the federal government may do in this particular area. I have no further comments on this.

Mr. J. Reid: Just to deal with our conclusion as set out in the paper, we believe that when you look at it from the point of view of trying to protect information as such, the problem is even bigger than we all initially felt. But we believe there has to be a first step, and our position would be that the first step would be to introduce a section dealing specifically with computers and dealing with their unauthorized use or access. We would certainly hope that the committee and Parliament generally would look upon this only as a first step, and would continue to try to upgrade our laws in dealing generally with information and its protection. That concludes our overview and we will be pleased to answer any questions or enter into discussion.

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman. I want to thank the three witnesses who have appeared before this subcommittee of the Standing Committee on Justice and Legal Affairs and for providing us with a great deal of interesting and informative information. I

[Traduction]

tion, car le tribunal a décidé, et nous pensons qu'il a eu raison, qu'un ordinateur n'est pas un service de télécommunication. Ce n'est pas la même chose.

Nous proposons d'ajouter au Code criminel un article distinct, si tout délit informatique doit être considéré comme une infraction criminelle, qui porte sur les systèmes informatiques. Voilà comment on pourrait résoudre le problème car en fait vous arrivez ainsi à circonscrire une chose en particulier. L'industrie de l'informatique a la réputation d'évoluer rapidement. Par conséquent, le Parlement devrait régulièrement étudier la question pour se mettre au diapason de cette évolution technologique, sinon la loi risquerait d'être rapidement désuète.

Il faut également, à notre avis, étudier la question des sanctions qui portent directement sur la question de la valeur de l'information protégée ou des pertes que son utilisation, son abus ou son vol entraînent. L'information en elle-même n'a que peu de valeur intrinsèque. Elle ne fait rien pour personne. Ce n'est que lorsqu'elle est utilisée qu'elle présente en fait une certaine valeur. En d'autres termes, si elle est utilisée au profit ou au détriment de quelqu'un, quel que soit le cas, il va vous falloir imposer une sanction en vue de protéger ce concept, et ce dans le but de dissuader ceux qui voudraient utiliser frauduleusement cette information. En d'autres termes, plus la victime subit un tort ou un inconvénient, et plus l'auteur du délit en tire avantage, plus la sanction imposée devrait être sévère. On créerait ainsi un facteur de dissuasion tout en établissant une sanction pour le crime lui-même.

Par conséquent, nous pensons qu'il est davantage justifié dans ce cas-là de se protéger contre le vol, ou l'utilisation non autorisée du temps-machine et de l'information que l'ordinateur renferme sur le plan pénal; il faudrait également légiférer en matière civile, ce que feront vraisemblablement les provinces, lorsque le gouvernement fédéral aura décidé des mesures à prendre dans ce domaine ou avant. Je n'ai d'autre à dire là-dessus.

M. J. Reid: Je voudrais maintenant passer à la conclusion que renferme notre mémoire; lorsqu'on se penche sur la question en pensant à la protection de l'information elle-même, le problème est encore plus vaste que nous ne l'avions tous pensé au départ. Mais nous estimons qu'il faut agir et la première étape constituerait à ajouter au Code criminel un article portant sur les ordinateurs et sur leur utilisation ou accès non autorisé. Nous espérons que le Comité et le Parlement le verront également de cet oeil et continueront à améliorer les lois portant sur l'information et sa protection. Voilà ce qui conclut notre survol de la situation et c'est avec plaisir que nous répondrons à vos questions ou que nous discuterons avec vous.

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président. Je voudrais tout d'abord remercier les trois témoins qui comparaitront ce matin devant ce sous-comité du Comité permanent de la justice et des questions juridiques de nous avoir fourni autant de renseignements intéressants. J'espère

[Text]

hope it will not disappear through somebody attaching a terminal to a telefax somewhere. As a matter of fact, if they got this information maybe it would be all for the better.

I noted particularly, I guess with Mr. Reid, who was the first speaker, I believe . . .

Mr. J. Reid: Yes.

Mr. Robinson (Etobicoke—Lakeshore): —that you mentioned marketing of business equipment and you mentioned every kind of equipment one could possibly think of including data processing equipment, but you shied away from mentioning the word "computer". Was this done on purpose? Is there some particular reason why you skirt this? Your paper is entitled "Discussion Paper on Computer Abuse", but you never mentioned the word "computer" at all.

Mr. J. Reid: One of the problems we have is trying to determine from time to time what is, and what is not, a computer. We refer to it as data processing equipment. One of the points which has been raised from time to time is how do you define computer. I guess the industry would say that the definition you make today will be out of date tomorrow, which seemed to beg the question: Do you need a definition of "computer"? We all know what a computer is when we see one. From time to time all we have to do is say, that is not a computer.

One of the problems is what we now call a hand-held calculator. A lot of those have the computing power of a lot of the early computers, and yet we do not think of a calculator as a computer.

Mr. Robinson (Etobicoke—Lakeshore): Have you considered possible definitions . . . or the possibility of defining some of these words now in the technology of this so-called computer age? Have you considered some definitions, and can you help the committee with this kind of thing—maybe not today, but maybe by putting on your thinking caps and coming back with something which might be helpful to the committee? I mean by way of definition of some of the concepts, I suppose, or whatever you want to call them, that we will have to be dealing with in due course. One of them, of course, is as you suggested, a definition for the term "computer". I suppose it also includes a definition of information, a definition of data, a definition of many many other terms that are batted around.

I recall when I was in social work I spent a year at a psychiatric hospital—not as a patient but in a different capacity—and we used to use terms like psychopath, paranoid, and whatnot, and everybody has a stereotype in their mind, I suppose, as to what a psychopath is. But when I started asking people for a definition of a psychopath I found that very few people had really a good idea of what it was all about. I recommend to people they read Fotheringham's article; and I do not mean the Fotheringham who writes as a syndicated columnist, but rather an article by Fotheringham who I think has the best item on psychopathy.

[Translation]

qu'ils ne disparaîtront pas, quelqu'un ayant eu la mauvaise idée de raccorder un terminal à un téléfax quelque part. D'ailleurs, s'ils ont cette information en main, ils s'en porteront peut-être mieux.

J'ai noté que M. Reid, le premier orateur . . . c'est bien cela?

M. J. Reid: Oui.

M. Robinson (Etobicoke—Lakeshore): J'ai noté, donc, que vous avez parlé de commercialisation d'équipement de bureau et vous avez cité tous les équipements possibles y compris le matériel de traitement de l'information, mais que vous n'avez jamais prononcé le terme «ordinateur». L'avez-vous fait délibérément? Pourquoi l'avez-vous omis? Votre document s'intitule: «Document de travail sur la criminalité informatique», mais vous n'avez jamais prononcé le terme «ordinateur».

M. J. Reid: Un des problèmes qui se pose, c'est que de temps à autre, nous devons essayer de déterminer ce qu'est et ce que n'est pas un ordinateur. Nous parlons en général de matériel de traitement de l'information. La question de la définition d'un ordinateur a été soulevée de temps à autre. L'industrie vous dira sans doute que la définition à laquelle vous arrivez aujourd'hui sera désuète demain et l'on peut alors se poser la question suivante: A-t-on besoin de définir ce qu'est un «ordinateur»? Nous savons tous ce qu'est un ordinateur lorsque nous en voyons un. De temps à autre, tout ce que nous devons faire, c'est dire: Cela n'est pas un ordinateur.

Ce que nous désignons maintenant sous le nom de calculatrice de poche pose un problème par exemple. Nombreuses sont celles qui ont la même puissance de calcul que de nombreux ordinateurs antérieurs et pourtant, nous ne considérons pas une calculatrice comme étant un ordinateur.

M. Robinson (Etobicoke—Lakeshore): Avez-vous envisagé de définir certains des termes que l'on retrouve dans cette ère soi-disant informatique? Avez-vous envisagé de définir certains de ces termes et pouvez-vous aider le Comité à le faire, peut-être pas aujourd'hui, mais en faisant parvenir plus tard vos notes au Comité? Je veux parler de la définition de certains concepts, je suppose, ou appelez-les comme voulez, que nous devons étudier en tant voulu. Il faudra sans doute en arriver à définir le terme 'ordinateur'. Cela comprend également, je suppose, une définition de l'information, des données et des nombreux autres termes qu'on nous assène tous les jours.

Je me souviens que lorsque j'étais travailleur social, j'ai passé un an dans un hôpital psychiatrique, non pas en tant que patient, rassurez-vous, et nous utilisions des termes comme psychopathe, paranoïaque et ainsi de suite, et je suppose que chacun a une définition stéréotypée de ce qu'est un psychopathe. Mais lorsque je me suis mis à demander aux experts une définition de psychopathe, j'ai constaté que très peu de gens avaient une idée bien précise de ce que c'était. Je recommande aux gens de lire l'article de Fotheringham, pas celui qui écrit une rubrique régulière, mais un autre qui a, à mon avis, écrit le meilleur article sur les psychopathes.

[Texte]

• 1610

But once again this is what we have to do: define it, know what you are talking about. Frankly, this committee is not clear on what we are talking about. We are using terms; we are bandying about words that we cannot really say we can stereotype as meaning something.

Now, what is a computer? Maybe it is a soft, woolly thing; or maybe it is a piece of machinery or, as you call it, a data processing equipment. Well, then I will ask you: What is data processing equipment? Is it a data bank, some place for keeping information? What is it? I think this whole question of definition is so fundamentally important and must be dealt with, and we will be looking to people like you to provide us with information that would be helpful.

The Chairman: Maybe, Mr. Dean, it is the other definition of computer from IBM.

Mr. Dean: Yes.

Mr. Kaufman: It is different than the one from Xerox.

Mr. Dean: My feeling is that in focusing on the definition of computer, you may be missing the point. Information can exist quite separate and distinct from computers. I think we have got to focus on the information, generally; and if you do, you get away from the need to define computer. But in saying that, proceeding with the second point, we are suggesting that the first point is to amend the Criminal Code. It would require a definition of the computer and computer system; and recognizing that it is difficult, we still think we will have to step up to it.

There has been considerable experience in the United States in developing definitions of computers. The trend there, I think, is to get away from a computer itself, which is in many people's minds the central processing unit or the piece of equipment that does the information processing, and include in the definition other pieces of equipment that do not do processing but that are part of the computer system, that might be accessed in the commission of any offensive action.

The definition of computer system probably can be done. We can commit to giving you examples of definitions for your review. You cannot tell whether or not they will be adequate down the road as the computer systems change. As technology changes, the definition may not be adequate.

At the moment, the popular thinking is that computers are devices... I am quoting from a judiciary subcommittee meeting held in the State of California, where they tried to come to grips with this. They said:

... is a device that performs logical, arithmetic and storage functions by electronic manipulation and includes any property and communication facility related to or operating in conjunction with such a device, but does not include an automated typewriter or any computer designed and manufactured for and which is used exclusively for routine

[Traduction]

Mais de toute façon, nous devons absolument définir ce que c'est afin de savoir de quoi nous parlons. J'ai franchement l'impression que le Comité ne sait pas exactement de quoi il est question. Nous nous servons de mots qui sont un galvaudés et nous ne pouvons pas vraiment leur donner une signification.

Donc, qu'est-ce qu'un ordinateur? Est-ce une petite boule duveteuse, une machine ou, comme vous dites, de l'équipement pour traiter les données? Je peux alors vous demander: qu'est-ce que l'équipement pour traiter les données? Est-ce une banque de données, un endroit où emmagasiner l'information? Qu'est-ce que c'est? Toute cette question de définition est d'une importance tellement fondamentale qu'il faut absolument la régler et c'est en faisant appel à des gens comme vous que nous pourrions obtenir des renseignements utiles.

Le président: Monsieur Dean, peut-être pourrait-on entendre l'autre définition des ordinateurs qu'en fait IBM.

M. Dean: Peut-être.

M. Kaufman: Xerox n'a pas la même définition.

M. Dean: J'ai l'impression que si vous vous attachez trop à définir l'ordinateur, vous passez à côté de la question. L'information peut exister comme une entité parfaitement distincte des ordinateurs. Nous devons donc nous attarder plutôt sur l'information en général. Ce faisant, vous n'êtes plus obligé de définir l'ordinateur. Néanmoins, nous croyons que la première étape serait d'amender le Code criminel. Il faudrait effectivement définir alors ce qu'est l'ordinateur et le système informatique et, sachant que c'est difficile, nous devons tout de même nous y résoudre.

Aux États-Unis, on a beaucoup tenté de définir l'ordinateur. Là-bas, on a tendance à s'éloigner de l'ordinateur lui-même qui, pour bien des gens, est l'unité de traitement centrale ou la machine qui traite l'information, pour ajouter à la définition d'autres morceaux qui ne traitent rien mais qui font tout de même partie du système informatique et dont on pourrait se servir pour commettre une infraction.

Il est sans doute possible de définir un système informatique. Nous pouvons nous engager à vous en donner des exemples que vous pourriez étudier. Vous ne pouvez pas être certain que la définition retenue restera valable si le système informatique change. Il se peut que la définition ne puisse s'adapter à l'évolution de la technologie.

En ce moment, on aime bien penser que les ordinateurs sont des appareils. Je vais vous citer un extrait d'une réunion d'un sous-comité judiciaire tenue en Californie et à laquelle on essayait justement de trouver une telle définition. Voilà ce qu'on y a dit:

... c'est un appareil qui exécute des fonctions logiques, des fonctions arithmétiques et de la mémorisation par manipulation électronique, et qui comprend tout appareil et dispositif de communication reliés à cet appareil ou fonctionnant conjointement avec lui, mais cela ne comprend pas une machine à écrire automatisée ni un ordinateur conçu et fabriqué exclusivement à des fins domestiques, familiales ou

[Text]

personal, family or household purposes, including a hand-held electronic calculator.

That is one state's deliberation on what the definition should be. That may or may not suit our purposes. With personal computers coming out and becoming more prevalent with the power of old-technology computers, which I think we would all recognize should be caught, maybe it is not such a hot idea to exclude personal computers. But I think we can look at technologically what is out there at a given point in time and come up with a definition that probably is suitable at that time. But it may not be suitable down the road. Computers may not work electronically in the future; they could work in different ways.

• 1615

So I think we should be focusing on this as a first step and perhaps move quickly onto the second step, which is how do we protect information whether it is on a piece of paper that might be on a finance minister's desk and somebody happens to take a picture of it, how do you protect that? That has nothing to do with computers.

Mr. Robinson (Etobicoke—Lakeshore): I see. Well, you have in effect a definition on page 2 of your statement when you say that data, in effect, is by definition information, knowledge, concepts, ideas and know-how, and to that you add also, all intangibles and abstractions. But is that not the short definition that you are given for . . . ?

Mr. Dean: That is the definition of information, I would not say that is the definition of computer.

Mr. Kaufman: I think part of the problem is, if I might, the term computer is perhaps a little bit more historic and archaic. As time goes on the concept of processing of data in a non-large computer sense is equally something that has to be dealt with and come to grips with.

For good reason I think John Reid did not refer to computers generally; he talked about data processing because the member firms of CBEMA, many of whom do not manufacture computers but would manufacture things, like our company for instance, word processing devices, or intelligent copiers, where you have an ability to store information on a mechanical device manipulated. And it would be equally offensive for somebody to go into a word processor that might be very narrow in its capacities and have it taken away just as if somebody would go into ones files. And that leads to the issue of dealing with information in its larger sense. We could say why would you want to take . . . ? A lot of people would take information that is in your files. It is equally important there. Just because it now has the benefit of being converted to electronic impulse which the current technology, perhaps it might be optical tomorrow, or some other technology I am not aware of, but the principle is still the same. So I think it would be, in our view, perhaps a mistake to focus on the concept of a computer per se. You would be better to use something more generic. Maybe initially it might be appropriate to have computer as your definition. But equally, you are quite right, you must define what it is we are talking about and I think the

[Translation]

routinières et personnelles, y compris une calculatrice électronique de poche.

Voilà le fruit des délibérations d'un État. Cette définition peut convenir ou non. Avec la sortie des ordinateurs personnels qui possèdent de plus en plus les pouvoirs des ordinateurs de première génération et, qui, de l'avis de tous, devraient être inclus dans la définition, ce ne serait peut-être pas une très bonne idée que d'exclure les ordinateurs personnels. Je crois toutefois qu'on pourrait examiner la technologie actuelle et rédiger à partir de cela une définition adéquate. Cela ne signifie pas qu'elle sera toujours aussi valable un peu plus tard. Il se peut que dans l'avenir les ordinateurs ne soient plus électroniques.

Je crois que cela devrait être notre première étape et que nous devrions passer rapidement à la seconde, c'est-à-dire à la façon de protéger l'information, qu'elle se trouve sur une feuille de papier sur le bureau du ministre des Finances que quelqu'un photographie malencontreusement, ou qu'elle se trouve dans un ordinateur.

M. Robinson (Etobicoke—Lakeshore): Je comprends. À la page 2 de votre exposé, vous donnez effectivement une définition quand vous dites que les données sont, par définition, l'information, la connaissance, les concepts, les idées et le savoir-faire, et vous ajoutez que ce sont là des réalités abstraites et intangibles. N'est-ce pas là la brève définition qu'on vous donne pour . . .

M. Dean: C'est là la définition de l'information mais pas de l'ordinateur.

M. Kaufman: Si vous permettez, je dirais que le problème est sans doute dû au fait que l'expression «ordinateur» est archaïque. Avec le temps, il faudra tenir compte du concept du traitement des données dans un petit ordinateur.

Je crois que John Reid a raison de ne pas faire allusion aux ordinateurs en général. Il a parlé de traitement des données parce que la plupart des entreprises membres de l'ACFEB ne fabriquent pas des ordinateurs mais des machines de traitement de mots ou des photocopieurs intelligents, capables d'emmagasiner de l'information à l'aide d'un appareil mécanique. C'est pourtant tout aussi mal de subtiliser de l'information dans une machine de traitement de textes aux capacités fort limitées que dans les dossiers de quelqu'un. Voilà ce qui nous amène au problème de l'information au sens large. Vous pourriez vous demander quel intérêt les gens peuvent avoir à prendre cette information? Mais des tas de gens aimeraient avoir l'information que vous avez dans vos dossiers. Cette information a autant d'importance dans la machine de traitement de textes que dans les dossiers. Ce n'est pas parce qu'elle est convertie en impulsions électroniques aujourd'hui, peut-être optique demain, ou même autrement, que le principe devrait être différent. À notre avis, ce serait donc une erreur de s'attarder seulement sur l'ordinateur en soi. Il vaudrait mieux utiliser un terme plus général. Au départ, il serait peut-être bon de parler de l'ordinateur dans votre définition. Vous avez raison de demander qu'on définisse ce dont il est question,

[Texte]

use of the term data processing is a more encompassing one. Or information processing perhaps is even better because that is, in a larger sense, what one is talking about.

Mr. Dean: On that point I might add that our paper was entitled "Discussion Paper on Computer Abuse" because that was the name or the title given to the CIPS seminar held last month, to which this paper was submitted, to add to that CIPS meeting. If we had had our preferences we would have preferred to call it a discussion paper on information abuse.

Mr. Robinson (Etobicoke—Lakeshore): Information abuse?

Mr. Dean: Yes, that is more consistent with our position.

Mr. Robinson (Etobicoke—Lakeshore): And then considering that this so-called computer, putting the word in quotes, is only part of the information?

Mr. Dean: Yes, and I believe that if you are going to focus on computer you should be focusing on computer systems and not computers per se, realizing that it is something that is good only at the moment you are looking at it. You cannot draw a definition of a computer or computer system that will cover you for the future.

Mr. Robinson (Etobicoke—Lakeshore): If I understand so-called computer crime correctly, there is the in-house taking of information; that is, by employees working for a company and they have access to the data bank or part of it, and most of the companies that I have spoken to personally tell me that in their own in-house security they only allow several employees to have bits of information or a key that opens part of the data bank only and that there is only a very select few who may be able to get additional information from the data bank that would cover several segments of what is contained in the data bank, and there may not even be anyone in the company, or maybe only one or two, who actually have access to all of it, who have the codes or the access keys to all of the information in the data bank. Now, is this usually the way they are set up in most companies for security?

Mr. Kaufman: I can speak for our company. Yes, you have a large data bank where you would have a central processing unit with terminals across the country. People can access the computer only by way of a devious security system, usually consisting of a password enabling you to go forward into the system. The idea is obviously to protect the whole data bank and let people have access to that information which they need to carry on their particular function. There is no need to have access otherwise. But that is part of the problem—there is no penalty if they access something illegally, or wrongfully, if you will.

Mr. Robinson (Etobicoke—Lakeshore): Because it is not an offence, per se.

[Traduction]

mais je crois que le terme «traitement des données» est beaucoup plus vaste que celui d'ordinateur. Il serait peut-être même préférable de parler de traitement de l'information.

M. Dean: À ce sujet, je voudrais ajouter que notre document est intitulé «Document de travail sur la criminalité informatique» parce qu'il a été présenté à l'origine à la conférence organisée le mois dernier par l'Association canadienne de l'informatique. Si nous avions eu le choix, nous aurions préféré lui donner le titre de document de travail sur la criminalité liée à l'information.

M. Robinson (Etobicoke—Lakeshore): La criminalité liée à l'information?

M. Dean: Oui, c'est plus conforme au contenu.

M. Robinson (Etobicoke—Lakeshore): Et cet ordinateur ne serait qu'une partie du tout que représente l'information?

M. Dean: Oui, et je crois que si vous voulez absolument vous attacher aux ordinateurs, vous devriez songer plutôt aux systèmes informatiques et non pas aux ordinateurs eux-mêmes car leur existence est assez éphémère. Vous ne pourrez pas trouver une définition d'un ordinateur ou d'un système informatique qui vous protégera à jamais.

M. Robinson (Etobicoke—Lakeshore): Si je comprends bien ces crimes informatiques, il y a d'une part les vols internes, c'est-à-dire par les employés qui travaillent pour la compagnie et qui ont normalement accès à la banque des données ou à une partie de celle-ci. La plupart des entreprises avec lesquelles j'ai eu personnellement des contacts m'ont dit avoir leurs propres mesures sécuritaires; par exemple, elles n'autorisent que quelques employés à avoir accès à certaines données seulement et très peu d'élus peuvent tirer des données supplémentaires qui recouperaient plusieurs segments de la banque. D'ailleurs, il arrive qu'une seule personne, quelquefois deux, aient accès à l'ensemble de la banque de données, c'est-à-dire qu'ils ont les codes ou mots de passe pour toutes les données emmagasinées. Est-ce courant dans la plupart des compagnies?

M. Kaufman: Je peux vous parler de ce qui se passe chez nous. Nous avons une grande banque de données qui se trouve dans une unité de traitement central et il y a des terminaux partout au pays. On ne peut avoir accès à l'ordinateur que si l'on est capable de franchir une barrière sécuritaire, généralement en donnant un mot de passe qui vous permet d'avoir accès au système. L'idée, c'est évidemment de protéger toute la banque des données et de ne laisser les gens avoir accès qu'à l'information dont ils ont besoin pour leur travail. Il leur est inutile d'avoir accès à autre chose. C'est d'ailleurs une partie du problème, car il n'y a aucune sanction imposée à ceux qui gagnent l'accès à quelque chose illégalement ou plutôt à mauvais escient.

M. Robinson (Etobicoke—Lakeshore): Parce qu'en soi, ce n'est pas une infraction.

[Text]

Mr. Kaufman: And you end up with a situation of... The only remedy as a company, of course, in that circumstance, would be to tell a person not to do it again. Fire the person. That kind of a thing. But on the other hand, if a person was trying to hurt the company severely, that kind of remedy is not sufficiently a deterrent factor. It does not do anything for anybody.

Just following along what John was saying before. We have to get the problem solved in bits and pieces, as opposed to trying to come to grips with the thing in its complexity. As we talk about, it I think one can see the degree of—where it can ramble through, encompass. The definition problem is a serious one and I would like to say that I think it is important that we end up, at some point, starting the process rather than trying to solve, if I can suggest it, the problem in its entirety. I do not think it can be at one time. There are too many different problems that arise. But one can start the process.

Essentially, the position that CBEMA is taking is that we would like to see a first step in that direction. However imperfect it will be, and I am certain that it will be imperfect, it will be better than having nothing at all.

Mr. Dean: Getting back to the thrust that I think you are taking, I can confirm that IBM does have ways of selectively isolating data so that, if you do not have the whole story, the part that you do have does not tell you very much. Those kinds of processes, passwords, encryption, cost to implement. We believe the degree of protection that the owner of a computer system with data bases—the degree of protection that the owner builds into the system should be left up to the individual owner. You could pay a lot and have the nearly perfect system, or you could pay very little and your data may be quite exposed.

We do not feel the approach that the legislation should take is to regulate or legislate standards. Failing the attainment of these standards, there would be no crime if somebody accessed the data. We feel if a person chooses to leave his house unlocked and somebody goes in and takes a piece of tangible property, that is theft. And we feel that concept should also apply to information that may be on a system that the owner has chosen not to protect with these devices and processes that are there.

Mr. Robinson (Etobicoke—Lakeshore): Are you not suggesting that it is only a crime if you leave your house unlocked and somebody takes a...

Mr. Dean: No. I am suggesting that it is a crime whether the house is locked or not, if without colour of right somebody enters the premises and takes something. I am suggesting that whether the house is locked or not is not part of the issue with respect to theft, nor should the degree of data security processes that are put on a computer system. That should not play any part either, in determining whether or not an information abuse or offence has been committed.

Mr. Robinson (Etobicoke—Lakeshore): When IBM is selling a computer service, and I will use that term for lack of a better term, do you sell a security package along with it?

[Translation]

M. Kaufman: Le seul recours d'une entreprise, dans ce cas-là, c'est de réprimander la personne en lui demandant de ne pas recommencer ou de la congédier. Si toutefois cette personne essayait de nuire grandement à l'entreprise, cette sanction ne la découragera pas. Cela ne rend service à personne.

Pour poursuivre dans la foulée de John, je dirais qu'il nous faut régler le problème petit à petit au lieu de vouloir s'attaquer à tout en même temps, car c'est trop complexe. Je pense qu'à force d'en discuter, on peut sentir tout ce qu'il faut faire. La définition pose un problème grave et je dirais qu'il est important de commencer quelque part à trouver des solutions au lieu de chercher à régler tout le problème. Je ne crois pas qu'on y parvienne en un seul coup. Cela soulève beaucoup trop de problèmes différents. On peut toutefois commencer quelque part.

Essentiellement, l'ACFEB voudrait qu'un premier pas soit fait. Même s'il est tout à fait imparfait, ce dont je ne doute pas, ce sera mieux que rien du tout.

M. Dean: Pour en revenir à ce que vous dites, il est vrai qu'IBM a des façons d'isoler certaines données de façon que la partie à laquelle vous avez accès ne vous apporte pas grand-chose. Mais les méthodes, comme les mots de passe et les chiffrements, sont coûteuses. Nous croyons qu'il faudrait laisser à la discrétion du propriétaire d'un système informatique avec des bases de données, le soin de déterminer le degré de sécurité nécessaire. Si vous payez très cher, vous pouvez avoir un système presque parfaitement protégé, mais si vous ne payez presque rien, vos données sont assez vulnérables.

Nous ne croyons pas que la loi devrait imposer des normes. Le cas échéant, ce ne serait plus un crime pour quelqu'un de forcer l'accès aux données d'une entreprise qui ne s'y serait pas conformée. Si quelqu'un pénètre chez un étranger et en ressort avec un bien, on considérera qu'il y a vol même si le propriétaire de la maison est parti sans fermer ses portes à clé. Ce devrait être le même concept pour l'information contenue dans un système, que le propriétaire ait choisi de la protéger ou non.

M. Robinson (Etobicoke-Lakeshore): Êtes-vous en train de dire que ce serait un crime seulement si on laisse sa porte ouverte et que quelqu'un...

M. Dean: Non. Je dis que c'est un crime que la porte ait été fermée à clé ou non. On ne tient pas du tout compte du fait que la porte ait pu ne pas être verrouillée pour déterminer s'il y a eu vol ou non; ce devrait être la même chose pour le degré de protection assuré aux données d'un système informatique. On devrait être complètement indifférent à cette sécurité pour décider s'il y a eu infraction ou non.

M. Robinson (Etobicoke—Lakeshore): Quand IBM vend un service informatique, si vous me passez l'expression, vend-elle en même temps des mesures de sécurité?

[Texte]

Mr. Dean: We have programs that do help to secure the information that is on a system. Some programs are more expensive than others. We also can advise and do, for a fee, our potential customers; with respect to what additional steps they may want to take. But in the final analysis it is up to the customer to decide what he wants. He has to determine whether or not what we have to offer meets his criteria.

Mr. Robinson (Etobicoke—Lakeshore): Where would the security package be in your sales priority pitch?

Mr. Dean: It is a fairly important part of the pitch. But it is up to the customer to decide how much security he wants to buy. We will sell computers with no security programs associated with them, if that is the customer's desire.

• 1625

Mr. Robinson (Etobicoke—Lakeshore): Do you people have any brochures that go along with the computer indicating the security steps that should be taken in-house and outside as well?

Mr. Dean: We have brochures that describe how our security packages work, but we do not purport to tell the customers what security is best for them. It is up to them to make the decision. They may decide not to buy the degree of security that we offer. There are other programming houses that offer programs that the customer may find better suit his purposes. The point is that we do not tell a customer what security he should have and that our security package will meet his requirements. It is up to the customer to make his own selection.

Mr. Robinson (Etobicoke—Lakeshore): Would it be fair to say that really it is not a selling point in selling your computers; this is something that has to be asked for by the customer; it is not something you are pushing? In other words, you are not trying to sell a security package ahead of your competitor. You are selling the product but not the security package. Is that not a fair statement to make?

Mr. Dean: No, I do not think so. Security is a very important aspect with respect to any computer sale and it is a subject that comes up, but the ultimate decision . . .

Mr. Robinson (Etobicoke—Lakeshore): Who brings it up?

Mr. Dean: We bring it up. The customers quite often bring it up too.

Mr. Robinson (Etobicoke—Lakeshore): You bring it up in the small print, I guess, do you?

Mr. Dean: These discussions usually take place long before any contracts are signed. By "small print" I gather you are talking about . . .

Mr. Robinson (Etobicoke—Lakeshore): Normally, when you are selling a computer, as I understand it, you go to a company and you hold yourself out as being able to do something for him. You have to be able to show him how he is going to be more efficient, more effective, and have a better

[Traduction]

M. Dean: IBM a des programmes qui peuvent aider à protéger l'information d'un système. Certains programmes coûtent plus cher que d'autres. Nous pouvons également conseiller nos clients éventuels et même prendre pour eux, moyennant rémunération, des mesures de sécurité complémentaires. Au bout du compte, c'est au client de décider ce qu'il préfère. C'est à lui de décider si nous pouvons lui offrir ce dont il a besoin.

M. Robinson (Etobicoke—Lakeshore): Mais dans votre réclame, quelle importance accorde-t-on aux programmes sécuritaires?

M. Dean: Une assez grande place. C'est néanmoins au client de décider du degré de protection qu'il veut se payer. Si le client le désire, nous pouvons lui vendre un ordinateur sans aucune mesure sécuritaire.

M. Robinson (Etobicoke—Lakeshore): Donnez-vous avec vos ordinateurs une brochure expliquant les mesures de sécurité que les entreprises devraient prendre pour se protéger de leurs employés et des gens de l'extérieur aussi?

M. Dean: Nous avons des brochures qui décrivent nos programmes sécuritaires, mais nous ne prétendons pas dicter à nos clients ce qui leur convient le mieux. C'est à eux de décider; ils peuvent même décider de ne pas acheter un programme aussi sécuritaire que celui que nous offrons. D'autres marchands de programmes peuvent offrir quelque chose qui convient mieux au client. Bref, nous n'imposons pas au client un programme sécuritaire donné sous prétexte qu'il répond à ses besoins. C'est au client de choisir.

M. Robinson (Etobicoke—Lakeshore): Serait-il juste de dire que ce n'est pas là pour vous un argument de vente; il faut que le client se renseigne de lui-même. Vous ne lui proposerez rien. Autrement dit, vous n'allez pas essayer de mousser votre programme sécuritaire par rapport à celui de votre concurrent. Vous vendez un produit, mais pas des mesures de sécurité. Est-ce que je me trompe?

M. Dean: Je le crois. La sécurité est un aspect très important de la vente de nos ordinateurs et le sujet est abordé fréquemment; toutefois, la décision finale . . .

M. Robinson (Etobicoke—Lakeshore): Qui soulève la question?

M. Dean: C'est nous. Les clients le font assez souvent également.

M. Robinson (Etobicoke—Lakeshore): Vous n'en parlez pas très fort, n'est-ce pas?

M. Dean: Ce genre de discussion a en général lieu bien avant que les contrats soient signés.

M. Robinson (Etobicoke—Lakeshore): Normalement, quand vous vendez un ordinateur, vous vous présentez à une société et vous prétendez pouvoir lui rendre service. Vous devez pouvoir lui montrer comment elle pourra être plus efficace, avoir un meilleur outil de mise en marché, avoir une meilleure

[Text]

marketing tool, better information and so on, and in effect be able to have a higher profit margin by taking your product. This is all very well, but we are beginning to realize that this kind of technology is way ahead of, say, the protection that maybe should go along with it. This is what I am concerned about.

If you are not doing it, why are you not doing it? If you are not doing it, I would suggest that you should be selling a security package.

I have gone to companies and they have a computer setup and they do not have the foggiest idea about security. They have a little Mickey Mouse in-house approach where they change their codes or a few people have certain codes and certain keys to the data bank and that is as far as it goes. They have not the foggiest idea that they should be changing these frequently or that they have to not only consider the in-house theft but the theft from outside.

I would like you to explain, if there is a company, the head office is in Montreal and they have another office in Toronto and they are communicating between the two offices, one computer to another, how you stop the theft there?

Mr. Dean: By encrypting, and we do have that as a package and we will make it available for a fee if a customer wants it. Quite often he does not.

Mr. Kaufman: It is a sequential kind of a thing, though, once you have looked at it, because as manufacturers or suppliers of the equipment the first thing you do is talk about what the thing can do. Then, subsequent to that, you talk about how you can protect what it is that you are storing or doing on the equipment. The two come together, but they come in a sequence. The customer really wants to understand first what the equipment can do. Subsequently, we do talk about the security packages which are available from the suppliers or other parties who have only a specialty in terms of providing that particular security.

Even if you have a security package, I think you have to look upon it as the lock on a house. You can get a very sophisticated lock on a house, but there is always going to be somebody who is able to break it. Therefore, it still does not change the principle. The person who wants to access that house to take something out without colour of right—that is still a crime that should be a crime. The fact that the person who has bought the house has not bought the most secure system should not necessarily be penalized as a result of that. There may be a variety of reasons why that person might not want to do that. Time has shown that people who buy computer systems now are becoming more and more aware of security, and that is one of the questions that comes up to be discussed early in the sequence of the marketing of the product. We do not hide the fact. Clearly, we talk about it. But I think one has to look at the sequence in which the matter is dealt with.

Mr. Robinson (Etobicoke—Lakeshore): You people have a...

The Chairman: I think Mr. Reid would like...

[Translation]

information, bref avoir une plus grande marge de profits si elle achète votre produit. C'est très bien, mais on commence à se rendre compte que ce genre de technologie est loin d'être aussi bien protégée qu'elle le devrait. Voilà ce qui m'inquiète.

Si vous ne faites rien contre cela, dites-moi pourquoi? Peut-être devriez-vous vendre vos programmes sécuritaires.

J'ai rencontré des sociétés qui ont un système informatique et qui n'ont pas la moindre idée de ce que sont les mesures de protection possibles. Elles ont des méthodes d'amateur. Elles changent les codes de temps en temps ou donnent certains codes ou certaines clés pour la banque des données à quelques personnes seulement et cela s'arrête là. Elles ne savent pas du tout qu'elles devraient changer les codes fréquemment et qu'elles doivent prévoir non seulement le vol par les employés mais aussi par des étrangers.

Si une compagnie a son siège social à Montréal et un autre bureau à Toronto et que les deux bureaux communiquent par ordinateur, comment pouvez-vous empêcher les vols?

M. Dean: En chiffrant les données. Il existe un programme que le client peut obtenir moyennant une certaine somme. La plupart du temps, il le refuse.

M. Kaufman: Vous savez, tout ne vient pas en même temps. Au départ, quand vous rencontrez les fabricants d'un équipement, vous commencez par parler de ce que l'équipement peut faire. Par la suite, vous parlez de la façon de protéger ce que contiendra la mémoire de l'équipement. Les deux vont ensemble, mais l'une après l'autre. Le client veut d'abord comprendre ce que les machines peuvent faire pour lui. Ensuite, nous discutons des programmes de sécurité que peuvent fournir les fabricants ou d'autres entreprises dont c'est là la spécialité.

De plus, dites-vous qu'un programme sécuritaire se compare à la serrure d'une maison. Même si vous faites installer une serrure très compliquée, il se trouva toujours quelqu'un pour la crocheter. Cela ne change donc rien au principe. Celui qui veut entrer dans votre maison pour y prendre quelque chose sans autorisation commet un crime. Ce n'est pas parce que le propriétaire de la maison n'a pas nécessairement acheté la serrure la plus sécuritaire qu'il doit être pénalisé. Le propriétaire peut avoir ses raisons pour ne pas avoir choisi cette serrure-là. L'expérience montre que ceux qui achètent des systèmes informatiques sont de plus en plus au courant des questions de sécurité et c'est maintenant l'une de celles qui est soulevée presque au début des pourparlers. Nous ne dissimulons rien. Nous en parlons franchement. Il ne faut quand même pas oublier que tout ne se fait pas en même temps.

M. Robinson (Etobicoke—Lakeshore): Vous avez...

Le président: Je crois que M. Reid voudrait...

[Texte]

• 1630

Mr. J. Reid: As a matter of fact, I was just going to bring up the point that Mr. Krofman brought up, and that is that we can build the locks, as we can build the locks, or if people get alarmed people can build the locks, for houses. If you, as an owner of that house, want to put the most sophisticated, razzle-dazzle lock system on your house, that is your prerogative. I, as a builder of that house, do not and cannot force you to do that. It is available, and if you want it you may have it. I guess that is the point we are making; the kind of security system that you want to put in place will depend on what you want to keep in your house.

The other thing that should be pointed out is that most of the time when there is a breakdown in security, if you will, it is because of human error. I think in one of the studies I read recently somebody did a survey of people who have password codes. In one of the brochures that went with the small terminals, there was suggested a password that could be used, as an example. It turned out that in something like 40% of the cases the people had used the password given as an example in the book. We can build the systems, but if people do not want to use them, they are not going to.

Mr. Robinson (Etobicoke—Lakeshore): No, but you are missing the point I am making.

You keep analogizing this to a house. Whoever heard tell of anybody buying a house that did not have locks and did not have keys to go with the locks, and so on? But you are selling data processing equipment, or computers, and you are not selling this lock with it.

Mr. J. Reid: We are selling the lock. There is security in the computer. It then becomes the degree of security that you want.

Mr. Robinson (Etobicoke—Lakeshore): Now you are telling me that it is a selling point, is it?

Mr. J. Reid: No, we are selling the computer. The computer, by itself, has a security system built into it. If you are asking what are we selling, are we selling computers or are we selling the best security system available, we would say that we are selling data processing equipment. We recognize that people are going to try to break into them, so we do have security systems, but I do not think any of us here would say that we were in the business of selling security systems.

Mr. Robinson (Etobicoke—Lakeshore): Maybe I could have one more question—maybe two.

One aspect that I wanted to ask you about a bit further was this whole question of the penalties that you talk about. You talk about sanctions and penalties against the offender. What exactly would you propose? What kinds of penalties are you talking about? You indicate the value to the owner and the value to the receiver of the information, but that is a monetary thing. It would normally apply to the civil consequences, I would assume, and not to the criminal consequences. If, in fact, as you have suggested here, there were to be an amend-

[Traduction]

M. J. Reid: En fait, je voulais soulever le même point que M. Krofman, nous pouvons placer des serrures sur les ordinateurs comme lorsque les gens s'alarment on peut aussi placer des serrures sur les maisons. Si vous, propriétaire de cette maison, voulez les serrures les plus sophistiquées et les plus raffinées pour votre maison, c'est bien votre droit. Mais moi, comme constructeur de cette maison, je ne peux pas vous forcer à les accepter. Je peux les mettre à votre disposition, et vous pouvez les acheter si vous le désirez. Ce que nous voulons dire en fait, c'est que le système de sécurité de l'ordinateur qui sera mis en place, dépendra de ce que vous voudrez y préserver.

Il faut se rappeler aussi que la plupart du temps toute brèche du système de sécurité est généralement causée par une erreur humaine. Je lisais récemment une étude sur un sondage de propriétaires d'ordinateurs qui utilisent des mots de passe. Dans une des brochures qui accompagnaient un petit terminal, on avait proposé un mot de passe comme exemple. Il s'avère qu'environ 40 p. 100 des gens avaient utilisé ce même mot de passe pour leur ordinateur. Nous pouvons construire les systèmes, mais si les gens ne veulent pas s'en servir, ils ne le feront pas.

M. Robinson (Etobicoke—Lakeshore): Non, vous ne comprenez pas ce que je veux vous faire remarquer.

Vous comparez toujours vos systèmes de sécurité à ceux d'une maison. Avez-vous déjà entendu parler de quelqu'un qui achetait une maison sans serrures, ou sans clés pour ces serrures, etc.? Or vous, vous vendez de l'équipement de traitement de données, ou des ordinateurs, mais sans serrures allant avec.

M. J. Reid: Nous vendons la serrure. L'ordinateur a un système de sécurité inhérent. Cela dépendra toujours de la sécurité que vous désirez.

M. Robinson (Etobicoke—Lakeshore): Alors vous me dites que c'est un article de vente, n'est-ce pas?

M. J. Reid: Non, nous vendons l'ordinateur, et l'ordinateur a déjà un système de sécurité intégré. Si vous nous demandez si l'on vend des ordinateurs, ou le meilleur système de sécurité sur le marché, nous vous dirons que nous vendons de l'équipement de traitement de données. Nous admettons que les gens essaieront de s'y introduire, donc nous ajoutons un système de sécurité, mais personne ici vous dira que notre affaire est de vendre des systèmes de sécurité.

M. Robinson (Etobicoke—Lakeshore): Peut-être pourrais-je avoir une autre question ou deux?

Je voulais aussi vous parler de toute cette question des peines à imposer pour les infractions. Vous mentionnez qu'il faut des sanctions ou des peines imposées contre le contrevenant. Que proposez-vous précisément? Quel genre de peines avez-vous à l'esprit? Vous dites qu'il faut indiquer la valeur au propriétaire et au bénéficiaire des renseignements, mais cela, c'est une question d'argent. Cela a rapport aux aspects civils du cas, pas aux aspects criminels. Si, comme vous le proposez, on devait modifier le Code criminel, c'est une toute autre

[Text]

ment to the Criminal Code, we are really talking about a different aspect of it, and I doubt very much that it is going to be a question of restitution of the \$10 million that you made by way of computer crime, or something of that nature, but rather... What is going to be the deterrent? You say a penalty for deterrence. I never met anybody yet who ever thought he was going to get caught when he perpetrated a crime. He would not do it if he thought he was going to be caught. I do not really know how much deterrence there is in penalties, but maybe you can tell us what kinds of penalties you are talking about that are going to be a deterrent.

Mr. Kaufman: Just as it is very difficult to determine what deterrence any kind of term of prison, for instance, would have for any crime, that does not mean you should not have a prison term for a particular crime. It varies with the nature of the crime.

The difficulty here is that we are seeking penal sanctions of some sort. We have not yet sat down to try to determine, in our own minds, what the recommendation would be—whether it would be six months, two months, six years, ten years, fifteen years. The point we are really making is that, whatever is selected, it has to be sufficiently tough, because the consequence of the abuse could be things like the destruction of entire data banks, where somebody could do it for a joke, or deliberately because they want to get revenge, or whatever the motive might be. If somebody were doing it as a joke, for instance, and would be concerned about being caught with a severe penalty—and in that person's mind it could be two years in jail that would be sufficient to deter him, for others, 20 years might, might not. At least there is something that is *prima facie* for a deterrent purpose. We do not know what that level would be. And I presume that those who would draft the legislation and provide you with the research and so on backing up what that recommendation might be, would suggest something fairly strong in relation to the kinds of penalties given or imposed for other offences such as theft of property over \$50 or over \$200. There is discretion given to courts. There might be a range for instance; you might say not more than five years or not less than six months, or not less than a week. We are not so much concerned with the exact amount, other than the fact that consideration needs to be given to what that deterrent level might be, recognizing that we will never achieve—I do not think one can ever achieve—a truly deterrent factor.

• 1635

Mr. Robinson (Etobicoke—Lakeshore): You have used only the term theft, but there are different aspects of it.

Mr. Kaufman: Yes, and I am using that in the generic sense. I am using that in the sense of abuse, destruction, unauthorized access to. You might make a distinction in the course of your recommendations, that an offence by somebody who steals a data bank for purposes of advancing his own cause would be different from somebody who goes in and plays around with the data bank and does nothing with it. There perhaps the deterrent factor might be something along the

[Translation]

chose, et je doute beaucoup qu'on exige la restitution de 10 millions de dollars de profits criminels obtenus par voie de l'ordinateur, mais plutôt... Que sera le moyen de dissuasion? Vous proposez une peine. Moi je n'ai jamais connu personne qui croyait se faire prendre lorsqu'il commettait un crime. Autrement, il ne le ferait pas. Je ne sais pas dans quelle mesure les peines imposées peuvent prévenir le crime, mais peut-être pourriez-vous nous dire quel genre de sanction ou de peine il est question dans votre mémoire.

M. Kaufman: Il est tout aussi difficile de déterminer quelle sera la valeur de dissuasion d'un terme de prison, pour quelque crime que ce soit, mais cela ne nous empêche pas d'attribuer un terme de prison pour un crime particulier, selon la nature du crime.

Nous croyons qu'il devrait avoir une sanction quelconque. Nous n'avons pas encore étudié, entre nous, quelle sera notre recommandation, si la peine de prison devrait être de six mois, deux, six, dix, ou quinze ans. Nous disons simplement que, quelle que soit cette peine, elle doit être assez sévère, car la conséquence d'un abus quelconque peut être la destruction des banques de données au complet, que ce soit fait par plaisanterie, ou bien expressément pour se venger, ou pour quelque autre mobile. Disons, par exemple, que quelqu'un veut faire une blague, si la peine est suffisamment sévère, disons deux ans en prison, cela peut suffire à l'empêcher, alors que pour d'autres, 20 ans n'y suffiraient peut-être pas. Au moins faut-il que cette peine serve de dissuasion. Nous ne savons pas à quel niveau l'établir. Mais nous supposons que les auteurs de la loi vous donneront la documentation nécessaire pour justifier leurs recommandations, ils suggéreront une peine assez sévère et proportionnelle aux peines imposées pour d'autres infractions comme le vol au-dessus de \$50, ou au-dessus de \$200. Bien sûr, les cours peuvent exercer une certaine discrétion. On pourrait établir une gamme de peines; par exemple, pas plus de cinq ans, mais pas moins de six mois, ou pas moins d'une semaine. Ce n'est pas la durée de la peine qui nous inquiète particulièrement, sauf qu'il faut tenir compte de sa valeur de dissuasion, sachant très bien que nous ne pourrions jamais, que personne ne pourra jamais vraiment éviter ou empêcher leurs crimes.

M. Robinson (Etobicoke—Lakeshore): Vous avez utilisé le mot «vol», mais il y a différentes sortes de vol.

M. Kaufman: Oui, je m'en sers dans son sens général. Je m'en sers dans le sens d'un abus, de la destruction, ou de l'accès sans autorisation. Peut-être devriez-vous faire une distinction dans vos recommandations, en fait quelqu'un qui vole une banque de données pour ses propres fins, commet un crime différent d'une autre personne qui pénètre simplement pour s'amuser et n'en tire rien. Par exemple, le facteur dissuasion pourrait être semblable à celui imposé pour la

[*Texte*]

lines for impaired driving; your first offence might be a slap on the wrist—escalating upwards.

Mr. Robinson (Etobicoke—Lakeshore): On my last question for this round, could you tell us why you suggest that there should probably be an amendment to the Criminal Code which would cover the situation, rather than have a special act of Parliament on computers per se? Is this because it seems easier to accomplish, and you will already have a lot of safeguards in the Code to go along with it.

Mr. Kaufman: Creating new statutes is sometimes a more difficult thing to do because you are trying to grapple with the problem in its entirety. That is where we see the biggest difficulty here; you can go a long time trying to come up with a solution, whereas there is a mechanism now to allow at least a beginning. And if it should turn out over a number of years after you have made some progress in this regard that it would entail taking it out of the Criminal Code and putting it into a special statute because you have a large enough body of things you want to deal with, fine. But at least, in my view, it is a start. There is a Criminal Code. There are other things similar to it, theft of a telecommunications facility or unauthorized use of a telecommunications facility would be an example. It would be the place to begin. That is the concern we have as an association—that there be a need to begin soon rather than later.

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman.

The Chairman: Committee colleagues, it is not the habit of a chairman or chairperson to ask questions, but since we have a minimal number of people and I will be participating in the drafting of the report, I just would like to know your views on the modification. I do not think you are touching very much that aspect in your brief about the Canada Evidence Act. What modification would you suggest? Do you think the actual law can deal with it and we can collect the evidence and, of course, be efficient if we have the right definition in the Code and so on. But do you think once we have the definition, it will be easy to track down the robbers or those who are committing infractions?

Mr. J. Reid: If you are asking if we think it will be easy to prosecute somebody, our answer would be no. It is going to be difficult. But it can be done in certain circumstances. Perhaps as we get smarter, we will find ways to make it easier. Our position right now is that it does not matter how difficult it is, you cannot do it. I guess what we are saying is that if there is something, yes, it may be difficult, but it can be done. Some of these examples are real live examples, and they have tracked down the people who were doing it. If there had been legislation, I guess if there had been a provision allowing for charges, they would have been made. Again, we are dealing with hypotheticals to some extent. But will it be easy? No. Can it be done? Yes, and it may be easier along the way.

The Chairman: I have another question. I do not remember which page it was in your document, but you refer to the fact—going to your customer and the people using comput-

[*Traduction*]

conduite en état d'ébriété; pour la première infraction, on est grondé, et la peine augmente avec le nombre d'infractions.

M. Robinson (Etobicoke—Lakeshore): Voici ma dernière question. Pourriez-vous m'expliquer pourquoi vous préconisez un amendement au Code criminel plutôt que d'exiger une loi spéciale du Parlement sur les ordinateurs mêmes? Est-ce parce que cela vous semble plus simple, et qu'il existe déjà certaines sauvegardes au sein du Code criminel.

M. Kaufman: Il est beaucoup plus difficile de faire adopter une nouvelle loi, car il faut à ce moment-là étudier le problème dans son ensemble. C'est la plus grande difficulté, on pourrait étudier longuement la possibilité de trouver une solution, tandis qu'il existe déjà un mécanisme qui nous permet de commencer immédiatement. Si dans quelques années, les progrès technologiques nous permettent d'enlever ces dispositions du Code criminel et d'écrire une nouvelle loi particulière, parce qu'on a suffisamment de données, on adoptera cette loi. Mais il faut un début quelconque au moins. Le Code criminel s'y prête bien. Il y a d'autres peines semblables au sein du Code criminel, comme le vol d'une installation de télécommunications, ou l'emploi sans autorisation d'une installation de télécommunications. Ce serait un début. C'est ce que cherche notre association, et ce qui nous préoccupe, c'est qu'en fait il faut commencer le plus tôt possible, plutôt que d'attendre à plus tard.

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président.

Le président: Cher collègues, ce n'est pas dans l'habitude du président de poser des questions, mais puisque nous sommes un nombre restreint d'interrogateurs, et que je participerai à la rédaction du rapport, je voudrais aussi vous poser des questions sur l'amendement proposé. Dans votre mémoire, vous ne semblez pas dire grand-chose au sujet de la loi sur la preuve au Canada. Quelles modifications proposez-vous? Croyez-vous que la loi actuelle suffira, et qu'avec les bonnes preuves, bien sûr, on pourra poursuivre un criminel, si on a une bonne définition dans le Code criminel. Croyez-vous qu'une fois la définition établie, il sera facile de retrouver les voleurs, ou ceux qui ont commis les infractions?

M. J. Reid: Si vous demandez s'il sera facile de poursuivre quiconque, non, ce n'est pas le cas. Ce sera toujours difficile. Mais on pourra le faire sous certaines conditions. À mesure que nous apprendrons, nous trouverons des moyens de rendre la poursuite plus facile. En ce moment, cela n'a aucune importance; si c'est très difficile, on ne peut pas poursuivre. Donc, nous disons, oui, c'est très difficile, mais on peut le faire. Nous avons donné des exemples de cas réels, où on a pu retracer le coupable. Et s'il y avait eu une loi, permettant de mettre en accusation ces personnes, on aurait pu le faire. Malheureusement, il s'agit de cas hypothétiques dans une certaine mesure. Est-ce qu'il sera facile de trouver des coupables? Non. Est-ce qu'on peut le faire? Oui, et ce sera de plus en plus facile.

Le président: J'ai une autre question. Je ne me souviens pas à quelle page de votre mémoire, mais vous avez mentionné au sujet de vos clients et des personnes qui utilisent les ordina-

[Text]

ers—do you have the feeling that the public aspect of the criminal court and criminal justice system...? Of course, everything is all in public and so on, and the damages or the balance of inconvenience of suing somebody who is stealing data... Even though we have then, of course, caught the person who committed the offence—right definition, everything in the Code—then how many companies will take the risk to damage their image and take someone to court?

• 1640

Of course, the compensation is not attached to the Criminal Code. They will not be paid back. They will have to go to another court for that. It is just to punish. Do you not think, even though we have a very efficient criminal law amendment, the company will still hesitate to use that mechanism to penalize someone who has infringed upon their rights by using their computer data banks?

Mr. J. Reid: We do not know. We believe that there is a deterrent factor; and we believe there will be prosecutions, because if there are prosecutions and they are successful, it would be our belief that it would be less likely other people would do it.

One of the examples that was not mentioned in our paper but has been brought up from time to time is about the various universities—or a couple of universities, anyway—whereby computer classes were, at one point in time, giving jugs of beer to the first person who could break the code on the university system, until someone pointed out that as professors maybe that was not quite the thing they should be teaching. But when there is no sanction, that is very easy to do. They say, so I get caught; so what? Who really cares? If there is some sort of sanction, maybe people will start to think twice about things like that.

That is basically our position.

Mr. Kaufman: You also should consider, I think, the situation as it exists today. There are companies or organizations that are defrauded by their employees, or theft occurs. The same kind of thought process would go through there as to whether the employee is to be prosecuted or not. The company may, for a variety of reasons, choose not to prosecute, such as public image and so on. In other cases, it might, for the very purpose of setting an example.

I think the same kinds of thought processes would occur with this kind of crime, and there would be no more or no less prosecutions being taken as a result of it; perhaps even more, given the potential that here an entire data bank could be destroyed by an employee who is disgruntled, as an example, or a third-party confederate coming in and stealing. You might want to take more action than simply having somebody stealing some money from your petty cash.

That is the importance of the deterrents. Just the fact of the prosecution is so immense that I think we probably would want to take more prosecutions. But at the very minimum, it would be no different today in terms of decision making, in my view.

[Translation]

teurs... Que pensez-vous du fait que tout ce qui se fait dans un tribunal criminel, ou au sein du système pénal, est rendu public? Il est vrai que tout est public, mais il y a les dommages et les inconvénients rattachés aux poursuites intentées contre quelqu'un qui a volé des données... Même si l'auteur du délit est arrêté, même si nous avons la définition juste et tout ce qu'il faut dans le code, combien de compagnies risqueront d'endommager leur réputation et d'intenter des poursuites?

Il n'est pas question, évidemment dans le Code criminel, d'indemnisation. Les compagnies ne seront pas indemnisées. Elles devront s'adresser pour cela à un autre tribunal, puisque celui-ci est là uniquement pour imposer des sanctions. Ne pensez-vous pas que, même avec un amendement très efficace du droit pénal, la compagnie hésitera encore à recourir à ce mécanisme pour punir quelqu'un qui l'a lésée en utilisant sa banque de données?

M. J. Reid: Nous ne le savons pas. Nous croyons au facteur de dissuasion; il y aura des mises en accusation et si elles donnent de bons résultats, nous croyons que moins de gens seront portés à enfreindre la loi.

Un exemple qui n'est pas mentionné dans notre mémoire, mais dont on a parlé à l'occasion concerne les diverses universités, ou quelques-unes d'entre elles du moins, où à un certain moment donné, pendant les cours d'informatique, on offrait des chopes de bière à la première personne qui réussissait à faire sauter le code du système de l'université, et cela a duré jusqu'à ce que quelqu'un remette en question l'enseignement dispensé par les professeurs. Mais quand il n'y a pas de sanction, c'est très facile. On se dit que ce n'est pas grave de se faire prendre, on se dit: qu'est-ce que cela peut bien faire? S'il y avait des sanctions, on y penserait deux fois avant d'agir.

Voilà essentiellement notre position.

M. Kaufman: Vous devriez songer aussi, je pense, à la situation actuelle. Des compagnies ou des organismes se font voler par leurs propres employés, ou sont victimes de vol. Il faudrait se poser la même question et se demander si l'employé doit être poursuivi. La compagnie, pour diverses raisons, peut décider de ne pas tenter de poursuites, pour sauvegarder sa réputation et ainsi de suite. Par contre, elle peut décider de poursuivre l'employé à des fins simplement exemplaires.

Je pense que la même chose s'appliquerait ici, et qu'il n'y aurait pas plus ni moins de poursuites, d'autant plus qu'il y a toujours la possibilité qu'un employé mécontent détruise toute une banque de données, par exemple, ou qu'une tierce partie vienne commettre le délit. Vous voudrez peut-être alors imposer des sanctions plus sévères que celles qui s'appliqueraient à une personne qui s'empare des fonds de la petite caisse.

Voilà l'importance des mesures de dissuasion. Les poursuites, à elles seules, sont si importantes que nous devrions probablement en tenter davantage. Mais, d'après moi, cela ne changerait pas pour autant le processus de décision.

[Texte]

Mr. Dean: I would like to say the only recourse for the company that experiences this kind of problem would be to lodge a complaint and proceed by way of prosecution. There is some suggestion in the way you posed the question that maybe there was a civil right of action, that the company could start a civil action and recover damages. That, at the moment, does not exist. There would have to be some change to the provincial laws to make that happen. That is the reason I cautioned earlier against the approach to amending the Criminal Code to extend the definition of property to include information, because then you would have property meaning one thing for criminal purposes and quite a different thing on the civil side.

The Chairman: Yes, I do realize it is provincial jurisdiction. But I was saying, if we do act and the provinces are also initiating some sort of changes and permitting people . . . I refer to the notion in the civil code of damages; and of course, maybe it is easier for me under 1053 . . . I say it might be easier; I am not familiar with the common law approach. But I just say to myself, when there is a damage you can prove, then you can ask for repairs. Usually, it is monetary compensation.

Mr. Dean: 1053, was that . . .

The Chairman: That is under the civil code.

Mr. Dean: The civil code, the CBC case against a tabloid or against the doctor . . .

Mr. Kaufman: Yes, that was part of . . .

Mr. Dean: . . . invasion of privacy was the issue there.

Mr. Kaufman: Yes, that is right.

• 1645

Mr. Dean: I understand. Is this against the tabloid, or against the doctor, where an invasion of privacy was the issue there?

Mr. Kaufman: Yes, that was the point.

Mr. Dean: Okay, I understand.

The Chairman: Are you aware, because it is your field, that in other countries, in other parts of the world—and I refer maybe to Japan or maybe other countries in Europe or of course the U.S.—which step have they taken? I mean, in that particular field, Canada is a small country compared to these countries; the number of datas, the number of information, whether it is in Japan or in the U.S., is fairly large and they have big data banks. What step are they taking?

Mr. Dean: I can only speak of what I believe is taking place in the States. About 16 states have attempted to legislate abuse of data processing systems, using the first step approach that we are recommending.

The Chairman: Do you mean the Criminal Code?

Mr. Dean: Having a provincial or state offence that is criminal in nature, although it may not be punitive, that uses

[Traduction]

M. Dean: Le seul recours de la compagnie qui est aux prises avec ce genre de problème serait de porter plainte et d'intenter des poursuites. Vous avez semblé demander s'il y avait un recours au civil, si la compagnie ne pouvait pas intenter une poursuite au civil pour obtenir un dédommagement. Il faudrait que des changements soient apportés aux lois provinciales. C'est la raison pour laquelle je vous ai invités à la prudence avant de préconiser des amendements au Code criminel visant à étendre la définition de propriété pour que cela comprenne l'information, parce que vous aurez alors une définition de propriété pour le criminel et une autre définition tout à fait différente pour le civil.

Le président: Oui, je comprends qu'il est question de compétence provinciale. Mais si nous adoptons des modifications et si les provinces en font autant et permettent aux gens . . . Je pense à la notion de dommages dans le Code civil; et il est peut-être plus facile pour moi évidemment en vertu du 1053 . . . Je dis qu'il serait peut-être plus facile, mais je ne connais pas tellement le système de la *common law*. Mais tout ce que je me dis, c'est que, quand on peut établir qu'il y a eu des dommages, on peut exiger un dédommagement. D'habitude, c'est un dédommagement monétaire.

M. Dean: Le 1053, c'est . . .

Le président: Dans le code civil.

M. Dean: Le code civil, Radio-Canada contre un journal de type *tabloid* ou contre le docteur . . .

M. Kaufman: Oui, c'était un élément . . .

M. Dean: . . . c'était une question d'intrusion dans la vie privée.

M. Kaufman: Oui, vous avez raison.

M. Dean: Il y a atteinte à la vie privée pour qui, le journal, le médecin?

M. Kaufman: Tout est là.

M. Dean: Je comprends.

Le président: Vous savez ce qui se passe ailleurs dans ce domaine, au Japon, en Europe, aux États-Unis? Vous savez quelles mesures ont été prises à cet égard? Le Canada n'est qu'un petit pays comparé aux autres. Que ce soit au Japon ou aux États-Unis, les banques de données, l'information doivent être beaucoup plus considérables.

M. Dean: Je ne suis au courant que de ce qui se passe aux États-Unis. Environ 16 États ont essayé d'adopter des mesures législatives contre l'abus des systèmes informatiques, en passant par la première étape que nous recommandons nous-mêmes.

Le président: Vous voulez dire le Code criminel?

M. Dean: En créant d'abord une infraction criminelle aux yeux de la province ou de l'État, même si cette infraction n'est

[Text]

the approach that defines a computer system and makes it an offence to improperly access it or to improperly use it.

The Chairman: If we were stealing, for instance, from Montreal with telephone line information in New York, how would you deal with that?

Mr. Dean: Sorry?

The Chairman: If I were stealing information through a telephone line in New York, how would I deal with that? I mean, I create the offence here. With telephones, and now with the sophisticated telecommunications, I can almost steal anywhere in the world. I mean, with the satellites and everything, and through telephones, if I have the code and I have the keys, I presume I can have access.

Mr. Kaufman: That is a significant issue. The question there is, where is the offence being committed, the part where it is accessed on the other side, or here? I do not think there is an answer that is easy. There are obviously international treaties which will have to be adopted with respect to this and that is not going to be a simple thing because of the vested interests of countries.

The Chairman: That was my question, yes.

Mr. Kaufman: But in any event, even if that—and that is again one of the reasons why we suggest rather than trying to grapple with all the main major areas, of which this is one, a first step, however small is that, it gets you towards that. I do not have an answer to your question, though, Madam Chairman, because it is a difficult one to answer. There is no easy solution to it.

Mr. Robinson (Etobicoke—Lakeshore): Several of you have suggested there could be a command given to the computer to self-erase or to destroy, but you have not indicated what you do to provide a safeguard for this. Far be it from me to tell you your business but surely you must have a backup system that you sell at the same time as you sell the front system.

Mr. J. Reid: You mean by a system, in that instance you are really destroying data and yes, if you duplicate your data you have your backup data that you are always going to be able to bring in. But you would lose all the data that was on the machine at that point in time that it did crash. As far as the system, if the system self-erases, sure you hopefully would have another system. But in that instance it is as if you yourself had gone out to hire somebody and said write me this system, and he wrote you that system. If he had built that protection for himself into it, if you had decided that you should duplicate that program for your files, then fine, you then have the program you can call back up. But if you did not do that then you are going to have to go out and hire somebody else to write another program for you.

Mr. Robinson (Etobicoke—Lakeshore): Is this something that you sell to your prospective customers, a backup system?

Mr. J. Reid: Yes, this is something customers, if you fail to deal with that issue, the first time the thing crashes they are

[Translation]

pas toujours assortie de mesures punitives, en définissant d'abord ce qu'est un système informatique et en déterminant que l'accès ou l'utilisation non autorisé est une infraction.

Le président: Si à partir de Montréal, par exemple, quelqu'un s'appropriait de l'information sur une ligne téléphonique à New York, quelle mesure pourrait être prise?

M. Dean: Je vous demande pardon?

Le président: Si je m'appropriais de l'information sur une ligne téléphonique à New York, qu'est-ce qui se passerait? Je commettrais l'infraction ici. Le téléphone et tous les autres moyens de communication perfectionnés me permettent de voler à peu près n'importe quoi dans le monde: il y a les satellites et bien d'autres choses encore. Si j'ai le code, c'est tout ce qu'il me faut. Je peux avoir accès au système.

M. Kaufman: La question est importante: il s'agit de savoir où l'infraction est commise, là où se trouve celui qui accède à l'information ou de l'autre côté. Il n'y a pas de réponse facile à cette question. Il faudrait évidemment que des traités internationaux soient conçus à cet égard. Ce ne sera pas chose facile parce qu'il y a des pays qui ont des intérêts dans l'affaire.

Le président: C'était le sens de ma question.

M. Kaufman: C'est pourquoi nous recommandons de commencer par le début, si modeste soit-il. Il ne faut pas essayer de régler tous les problèmes à la fois, et celui que vous évoquez est l'un des plus importants. Je ne sais trop comment vous répondre, madame le président. Votre question est loin d'être facile.

M. Robinson (Etobicoke—Lakeshore): Plusieurs d'entre vous ont fait allusion à un commandement qui pourrait être donné à l'ordinateur pour qu'il s'autoefface ou s'autodétruit. Vous n'avez cependant pas parlé de garantie à cet égard. Il ne m'appartient évidemment pas de vous dire ce que vous avez à faire, mais je suppose que vous devez avoir un système d'appoint lorsque vous vendez un premier système à un client.

M. J. Reid: Par là vous voulez dire qu'au cas où vous seriez amené à détruire vos données vous établissez un double de ces données auxquelles vous pouvez toujours avoir recours. Il n'en demeure pas moins que toutes les données qui se trouveraient dans l'ordinateur seraient détruites au moment où il casserait. Dans le cas d'un système qui s'autoeffacerait, vous pourriez avoir un autre système. Mais dans ce cas, c'est comme si vous aviez embauché quelqu'un pour doubler le système. Il y aurait alors introduit cette protection. Vous auriez alors un double pour vos dossiers. Vous pourriez toujours compter sur ce programme. Mais comme je l'ai dit, il faudrait avoir demandé à quelqu'un de vous préparer un tel système.

M. Robinson (Etobicoke—Lakeshore): Vous essayez de vendre un tel système d'appoint à vos clients éventuels?

M. J. Reid: Si vous ne le mentionnez pas la première fois à vos clients, la première fois que le système est en défaut, vous en entendez parler.

[Texte]

looking to you. It does not pay not to bring it up. It is brought up, yes.

Mr. Robinson (Etobicoke—Lakeshore): It is not just to avoid the criminal aspect of it or the theft or misuse of information, but also your own employees may make a mistake, erase something or destroy something by mistake, so I would think there would be a backup at all times.

• 1650

Mr. Dean: Recovery, backup systems are addressed, and then again it is for the customer to decide how much he wants to spend on this kind of arrangement. You should not, I think, restrict that subject to the data bases and the programs. Also included in the subject is the hardware itself. If you have a fire and the physical asset is destroyed, how do you recover? It is an interesting subject, but I am not sure I completely understand what it has to do with information abuse. I have been trying to see where you are going.

Mr. Robinson (Etobicoke—Lakeshore): I think preventive measures are always in vogue. At least, hopefully, we are not just looking at setting up a criminal procedure and making computer theft a crime and having penalties and so on. Why do we not try to avoid it? That is what I would like to know from you people: What are you doing to try to avoid computer theft or computer crime? That is why I am asking you about security packages, backup systems and so on. There must be something that you are doing in this way to avoid this kind of thing because obviously at some stage your customers are going to say: What about this? What are you going to do to protect the information I am putting in the data bank? What do I have to do—put it in the vault every night?

Mr. Kaufman: These are all there. It is a current state of the art. The systems are there. The difficulty that exists is that much of the security system is created on software, the programming of this, and people who wish to and who are knowledgeable can get around it. There is never a foolproof system. There just cannot be. You can make it as tight as you want; somebody who is determined will break it eventually. There is no encryption that you can ever develop, I think—at least I have never heard of any—that will be foolproof.

While destruction is an issue and we do address it by providing information on the kinds of security systems that you have in place to prevent that, what about those who deliberately seek to go through the maze? That will never stop them. They may not get in there today, but they will eventually work at it, and if they are smart enough—and there are plenty of them who are smart who would do this, some for malicious reasons, others for the joy of it, just the intellectual challenge of trying to break it, then inadvertently, as a result of breaking it, destroying some data—not deliberately. One has to capture that side as well, without in any way saying we are not worried about security.

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Il ne s'agit pas seulement de se protéger contre des infractions criminelles, le vol ou la mauvaise utilisation de l'information, mais également contre les erreurs que pourraient commettre les employés. Ils pourraient effacer des données par erreur, par exemple. Selon moi, il devrait toujours y avoir un système d'appoint.

M. Dean: Les systèmes de recouvrement, d'appoint, sont offerts, mais il appartient toujours au client de décider du montant qu'il veut dépenser pour ces mesures. Par ailleurs, ce genre de protection ne doit pas exister seulement pour les banques de données et les programmes. Elle doit être offerte pour le matériel. Si vous êtes victime d'un incendie et que votre matériel est détruit, comment procédez-vous? C'est un sujet très intéressant, mais je ne vois pas tout à fait ce qu'il a à voir avec l'abus des systèmes informatiques. Je dois vous avouer que je ne vois pas très bien où vous voulez en venir.

M. Robinson (Etobicoke—Lakeshore): Les mesures de prévention sont très en vogue. Il est à espérer que notre préoccupation ne sera pas seulement d'établir une procédure criminelle et de créer une infraction criminelle pour le vol lié aux ordinateurs, le tout assorti de peines. Nous devons avoir recours à la prévention. C'est pour cette raison que je vous demande ce que vous faites pour empêcher le vol et le crime liés aux ordinateurs. Je veux savoir si vous avez des systèmes de sécurité et des systèmes d'appoint. Il doit y avoir quelque chose que vous pouvez faire pour éviter ce genre de situation. Vos clients doivent vous interroger à ce sujet. Ils doivent être intéressés de savoir ce que vous faites pour protéger l'information qui se trouve dans les banques de données. Qu'est-ce qu'il faut faire? La garder dans des chambres fortes?

M. Kaufman: Nous faisons appel aux systèmes les plus perfectionnés. Il en existe. Le problème est que la plus grande part des systèmes de sécurité est orientée sur la programmation, de sorte que les gens qui en ont le désir et qui ont les connaissances nécessaires peuvent les contourner. Il n'y a évidemment pas de système à l'épreuve de tout. Vous pouvez concevoir le système le plus perfectionné. Il y aura toujours quelqu'un qui sera prêt à le déchiffrer. Il n'y a pas de codes, si perfectionnés soient-ils, qui résistent à tout.

Donc, la destruction est toujours possible, et nous essayons d'indiquer à nos clients quels sont les systèmes de sécurité disponibles. Cependant, il y aura toujours ceux qui essaieront délibérément de trouver la clé du mystère. Rien ne les arrêtera. Ils ne réussiront peut-être pas aujourd'hui, mais un jour ou l'autre, ils y parviendront, s'ils sont suffisamment intelligents. Il y en a beaucoup qui ont les connaissances nécessaires pour y arriver, pour quelque raison que ce soit, par malice ou pour le simple plaisir, pour le défi intellectuel que le problème pose. Il se peut qu'en cours de route ils détruisent par accident une certaine partie des données. Il faut essayer de faire quelque chose pour résoudre ce problème, même si le côté sécurité ne doit pas être négligé non plus.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): I agree with what you are saying, but it seems to me that our focus is really in the wrong direction.

We are talking about closing the barn door after the horse has been stolen. What I am trying to do is . . . What are we doing to keep the horse from being stolen? You have him tied up and you have the barn door locked and you have an alarm system that goes off and so on, so it is highly unlikely that somebody is going to try to steal the horse. I think you have to do the same thing with your information in your data bank.

Mr. J. Reid: If I may intrude here for a minute, we have banks that have vaults and safes and elaborate alarm systems, but there is always somebody who decides that he wants to go after \$10 million and he is going to do it. I guess that is what we are saying, too. Sure, we build these things in there and we can take certain steps and we can take very elaborate steps, but it is the same thing. In one instance he is going after \$10 million because it is cold, hard cash; in the other instance he is going after \$10 million in information.

Mr. Dean: The Criminal Code at the moment does not purport to describe the degree of security that banks must use to safeguard their money before a person can be successfully prosecuted for stealing money from a bank. The banks do have procedures. I am sure they vary one from the other. Some may be better than others. There is a cost associated with that. That, to date, has not been the subject of regulation. Whether the banks implement the best system in the world or the worst system in the world, if somebody goes in and steals then the issue is theft of the property and not the degree of security. I suggest that it is a worthwhile topic but not one that should take up the prime focus of this committee.

• 1655

The Chairman: I would like maybe to add to that and ask you a question. What is the difference, for instance, between what we are talking about—and of course we are more or less having the picture of high technology and the image of a very sophisticated system, and so on—and someone just spilling ink on Shakespeare's or Einstein's notes? In both cases it was valuable information to Einstein or to Shakespeare—if it was a manuscript of Shakespeare of a fantastic play that had been written—and somebody else, on purpose, just spilled ink on it and, of course, it disappeared.

I make that image so that we are not taken up by the technological aspect of it and we can try to find the mechanism for the solution to that problem of, first of all, taking away the information from the person who owns the information and, of course, the person also who has paid for that information—because it is not always the same person.

If I work for a company and I am a programmer, or an analyst, and I have developed a sophisticated program I might not own it, even though I have developed it, and so on, but you cannot steal it from the brain of the person who conceived it. How do we treat the person, for instance, who has worked in a company and has developed a very sophisticated program and is leaving with it and using it elsewhere, compared with the

[Translation]

M. Robinson (Etobicoke—Lakeshore): Je suis bien d'accord avec vous, mais il me semble que notre orientation est mauvaise.

Nous nous contentons d'essayer de réparer les pots cassés. Ne faut-il pas commencer par essayer de faire en sorte que les pots ne soient pas cassés? Si toutes les précautions nécessaires ont été prises, il est peu probable qu'un accident se produise. Je pense que vous devez procéder de la même façon pour l'information contenue dans vos banques de données.

M. J. Reid: Permettez. Nos banques sont dotées de chambres fortes, de coffres-forts et de systèmes d'alerte perfectionnés. Cependant, il y en a qui sont toujours prêts à voler 10 millions de dollars et qui réussissent. C'est ce que nous essayons de vous faire comprendre. Nous pouvons prendre toutes les précautions imaginables, il y a toujours un risque. Dans le cas des banques, la motivation est l'argent, les 10 beaux millions de dollars. Dans notre cas, c'est 10 millions de dollars d'information qui intéressent le voleur.

M. Dean: Le Code criminel ne prescrit pas les mesures de sécurité que doivent prendre les banques avant que quelqu'un puisse être poursuivi pour y avoir volé de l'argent. Il n'en demeure pas moins que les banques suivent certaines procédures. Elles peuvent varier de l'une à l'autre. Il y en a de bonnes et de moins bonnes. Il faut toujours compter avec les coûts. Mais, jusqu'à présent, on n'a pas jugé bon de réglementer cet aspect de la question. Que les banques aient les meilleures ou les pires mesures de sécurité au monde, lorsque quelqu'un y vole de l'argent, toute la question porte sur ce vol et non sur l'efficacité des mesures de sécurité. Donc, même si c'est un sujet très intéressant, je ne pense pas qu'il soit le plus important pour le Comité.

Le président: Je voudrais vous poser une question supplémentaire, si vous le permettez. Quelle est la différence entre ce genre de situation—nous parlons évidemment ici d'une technologie avancée, nous sommes en présence de systèmes très perfectionnés—et le cas de quelqu'un qui renverserait de l'encre sur les notes de Shakespeare ou d'Einstein? Dans un cas comme dans l'autre, il s'agit d'une information qui n'a pas de prix. Si quelqu'un renverse de l'encre délibérément sur un manuscrit de Shakespeare ou d'Einstein, cette information disparaît.

J'utilise cet exemple pour que nous nous éloignons de l'aspect technologique, pour que nous essayions de trouver une solution au problème qui consiste à priver de son information la personne qui y a droit, que cette information soit sienne ou qu'elle l'ait achetée, il peut y avoir une différence.

Si je travaille pour une société et que je sois programmeur ou analyste, je peux contribuer à établir des programmes très perfectionnés, mais je n'y ai pas droit. Par ailleurs, il est évident qu'on ne peut pas enlever du cerveau d'une personne l'information qu'elle a conçue. Que faire dans le cas d'un personne, par exemple, qui a travaillé pour une société, qui élaboré des programmes très perfectionnés, qui quitte so

[Texte]

one, of course, who has paid for it and someone else arrives and is replacing that person and just making a copy of it but has not participated in the development of it? The two can just commit an infraction; one would be, of course, that of using something. Someone like you knows how valuable the program could be. It could have taken two or three years to develop, with a big team. But it is so easy to make the prints of that program and to get a copy of it.

How do we protect that? For me, you can steal the information, misuse the information, but these valuable programs that are being developed by all the industries, and so on, and some of them are of a very highly scientific content, how do we protect that? Even though we create an offence, how do we describe the offence? There is intellectual property, there is the value to the company because they sell the services attached to that program. I am asking because we seem to deal with it on more of a global approach, but there are many steps that we have to deal with. I just say to myself, do we use only the Criminal Code to do that?

Mr. Kaufman: There are significant issues that you raise there, and it is necessary to deal with it on the civil side as well because there are remedies that could be available, are available and might have to be made available, such as injunctive relief, to stop somebody from using his information. It is very difficult, and the courts, in some cases, already have suggested . . . employees walking away with information. How do you take it out of a person's brain? It is a very difficult concept.

On the other hand, if it is a program that has been developed and belongs to somebody and you sign, for instance—and this is something a company might have to do—a contract that says, I have developed it and it does not belong to me, and then you go elsewhere and, because it is in your brain, you transform it back into a program, I would suggest that the law needs to address the civil issue with injunctions. That is in the province's jurisdiction, perhaps. I think the question of deterrence is important here from a criminal law point of view. That may stop them from doing that.

There is always going to be a line that is hard to draw, or step over and figure out where it is you have to stop. I do not have an easy answer—I do not think you have either, nor does anybody, really—on dealing with that. It seems to me that, in the example you give, I would like to see that deterrence to that person. I would like to be able to do something in that case, because I paid the person to do what the person has done, the person has done it on my time on my equipment, and I have bought his brains, or her brains, for that purpose and it is now my property. If they are taking it away I wish to have a remedy. To the extent that I do not have that today, that is, I consider, very unfortunate, but that does not mean it is right.

• 1700

I think the step with respect to computers is that if he does or she does, take it away that way, the fact that having a

[Traduction]

employeur et utilise cette information ailleurs? De même, que faire dans le cas d'une personne qui fait une copie de l'information à l'élaboration de laquelle elle n'a pas participé? Dans les deux cas, il peut y avoir eu infraction. Premièrement, on a pu utiliser quelque chose auquel on n'avait pas droit. Vous savez sûrement la valeur que peuvent représenter certains programmes. Il se peut qu'il ait fallu à une équipe deux ou trois ans de travail pour y arriver. Il est si simple d'en faire une copie.

Comment vous protéger contre ce genre de chose? S'il convient de parler du vol et du mauvais usage de l'information, que dire de tout ce qui peut arriver à ces programmes très précieux qui ont été élaborés par des industries et qui contiennent des renseignements très techniques? Si nous voulons créer une infraction pour ce genre de chose, comment la décrire? Nous pouvons peut-être parler de propriété intellectuelle, de la valeur de certaines informations pour les sociétés qui vendent les services qui y sont rattachés. Nous semblons toujours rester sur le plan général, alors que selon moi il y a beaucoup d'étapes à franchir avant d'en arriver à une solution. Je me pose d'abord la question: Est-ce que nous devons avoir recours au Code criminel?

M. Kaufman: Vous soulevez un certain nombre de points très importants. Il faut prévoir des poursuites civiles également. Il y a déjà des solutions à un certain nombre de ces problèmes, il pourrait y en avoir d'autres, par exemple, les injonctions, pour empêcher certaines personnes d'utiliser l'information. Il n'en demeure pas moins que ce sont des choses qui ne sont pas faciles à établir. Par exemple, il y a le cas des employés qui emportent avec eux des informations. Comment les en empêcher?

Il se peut qu'un employé ait établi un programme, il peut avoir signé une entente, les sociétés y auront peut-être recours davantage, disant que même s'il a participé à son élaboration il n'y a pas droit. Cependant, s'il va ailleurs, il peut utiliser les connaissances qu'il a. Il peut les transformer en un programme. À ce moment-là, il y a toujours le recours aux injonctions devant les tribunaux civils. Je pense que c'est de compétence provinciale. Il reste le facteur de dissuasion que peut représenter une infraction criminelle. Ce peut-être suffisant pour empêcher les abus.

Il serait évidemment toujours difficile de faire la part des choses. Je n'ai pas de solution facile à vous proposer. Je ne pense pas qu'il en existe. Pour ce qui est de l'exemple que vous citez, madame le président, je souhaiterais qu'il y ait un moyen de dissuasion quelconque pour empêcher une telle personne d'agir. Je voudrais avoir un recours quelconque, parce que j'aurais payé cette personne pour le travail qu'elle a fait. Cette personne aurait utilisé mon temps et mon matériel. J'aurais payé pour ses connaissances. Les résultats obtenus seraient ma propriété. Il faudrait que j'aie quelque chose pour défendre mon bien. Pour l'instant, je suis privé de tout recours, mais cela ne veut pas dire que c'est juste.

Le fait qu'il existe une infraction criminelle dans ce genre de situation pourrait être suffisant pour empêcher quelqu'un

[Text]

deterrent, such as a criminal penalty, might cause somebody to think twice about doing that. The question of proof always arises when they go ahead and misuse that information. How can we prove in fact, what they are doing is the same thing as what we have them do for us? I guess that is why we all have lawyers.

The Chairman: Okay. You see the challenge that is facing us in trying to tackle this problem within—actually the spirit of the Criminal Code. It is a very specific law and we have to really have a good definition, of course, to make sure that we do not create more problems rather than solve problems. Do you have one last question? It is 5.00 p.m., Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Yes. You state in your paper:

The nature of data itself combined with computer technology enable one to acquire knowledge of another's data without depriving him of it nor leaving clues of his accessing it.

And this brings up the whole question of, first, what we would call, instead of in-house theft, outside theft . . .

An hon. Member: Outhouse theft.

Mr. Robinson (Etobicoke—Lakeshore): Well, maybe outhouse theft. And the other thing is, should it not be a crime not to report the so-called computer crime, if it occurs in your corporation? First of all, it may go undetected and of course you cannot do anything about that, because you do not know about it. But if it is detected, should it not be an onus on the company to make note of this and see that charges are laid? Should that not be part of the amendment to the Criminal Code as well? And also, after you answer that, would you indicate to me how the outside theft could take place, if it done within the corporate premises themselves?

Mr. Dean: Well, on the first issue, it is not a requirement, under our current Criminal Code, to report the commission of a crime. So to introduce that element to the information abuse would be a radical departure from the current set up of the Criminal Code. It is possible but it would be a first. You would be breaking new ground.

Mr. Robinson (Etobicoke—Lakeshore): I just thought from the statement you make here that the reason they do not report is because of bad publicity and other possible exposures. You might never get anybody reporting a crime at all. Why have an amendment to the Criminal Code if it is not going to be effective?

Mr. Kaufman: If the owner of that particular information is prepared to not report it and suffer the loss and deal with that, I think it is a private decision. If, on the other hand, as a parliamentarian, you are prepared to make this a matter of public order, such that society is so endangered by this failure to report, that is another issue. I think, as Mr. Dean has mentioned, it is a question then of breaking some new ground. Maybe it is necessary. I do not express a view one way or the other. It just seems, to my way of thinking, that we have a

[Translation]

d'agir. La question de la preuve est toujours soulevée lorsqu'il s'agit d'un cas de mauvais usage de l'information. Par exemple, comment prouver que ce que fait maintenant l'ancien employé est la même chose que ce qu'il faisait auparavant? Je suppose que les avocats sont là pour poser de telles questions.

Le président: Vous voyez quelles difficultés nous attendent si nous voulons essayer de régler ce problème en faisant appel au Code criminel. À ce moment-là, il faut que nous soyons très précis et que nous ayons de bonnes définitions. Nous devons essayer de résoudre des problèmes, pas d'en créer de nouveaux. Vous avez une dernière question? Il est 17 heures, monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Dans votre mémoire, vous dites ce qui suit:

La nature des données, de même que les techniques informatiques, permettent d'acquérir des connaissances figurant dans les données d'une autre personne sans en priver cette dernière, ni laisser de traces.

C'est toute cette question, non plus du vol de l'intérieur, mais du vol de l'extérieur . . .

Une voix: De l'extérieur.

M. Robinson (Etobicoke—Lakeshore): Et à cette question, s'ajoute celle-ci: le fait de ne pas signaler une prétendue infraction relative aux ordinateurs, commise chez une société, devrait-il être aussi une infraction criminelle? Évidemment, si l'infraction n'a pas laissé de trace, il est impossible de faire quoi que ce soit. On ne s'en aperçoit même pas. Cependant, si elle est décelée, la société impliquée ne doit-elle pas en prendre bonne note et engager des poursuites? Ce dernier fait ne doit-il pas être inclus dans l'amendement au Code criminel? Deuxièmement, comment un vol par quelqu'un de l'extérieur pourrait-il avoir lieu s'il est commis dans les locaux de la société impliquée?

M. Dean: D'abord, personne n'est obligé actuellement de signaler une infraction en vertu du Code criminel. Introduire cet élément dans le cas de l'abus des systèmes informatiques serait aller directement à l'encontre des principes contenus actuellement dans le Code criminel. Ce serait sûrement un précédent.

M. Robinson (Etobicoke—Lakeshore): Il me semblait que vous aviez dit que la raison pour laquelle certaines sociétés ne signalaient pas les infractions était qu'elles craignaient la mauvaise publicité et toutes sortes de révélations. Il se peut après tout que les sociétés décident de ne pas signaler les infractions. Pourquoi modifier le Code criminel si les mesures doivent être inefficaces?

M. Kaufman: Si le propriétaire de l'information décide de ne pas signaler l'infraction et d'absorber les pertes sans rien dire, libre à lui. En ce qui vous concerne, en tant que parlementaire, vous devez vous intéresser à l'ordre public, vous devez veiller à ce que la société ne soit pas menacée par ce défaut de signaler l'infraction. C'est une autre question. Comme M. Dean l'a indiqué, c'est un domaine tout à fait nouveau. Il se peut que des mesures soient nécessaires. Personnellement, je ne suis ni pour ni contre. Il me semble seulement que notre façon

[Texte]

precedent, the way we do things now, that seems adequate. That this could be one more type of an offence with that kind of an approach, without saying, it might not be necessary to go that step further. I do not see the argument just yet.

Mr. J. Reid: I think if you were considering doing the computer information abuse, you would have to look at extending it across the board. There are lots of embezzlers, I think, who do not get reported by their employers. That is a different offence entirely. It is an interesting subject, but I think it goes beyond the computer abuse. Could you repeat the second part of your question? We were not just entirely sure what you were asking there.

Mr. Robinson (Etobicoke—Lakeshore): Well, in my view, there may be a difference between what is considered as inside theft or computer abuse. There is also outside theft or computer abuse.

Mr. J. Reid: Do you mean by somebody who is not an employee? Someone who is doing it from a remote location.

Mr. Robinson (Etobicoke—Lakeshore): Yes.

Mr. J. Reid: Yes. Okay.

Mr. Robinson (Etobicoke—Lakeshore): I suppose they have to have a terminal someplace to be able to get into the computer.

Mr. J. Reid: Yes.

Mr. Robinson (Etobicoke—Lakeshore): But this could be done from any place. Across the street, in the next building or something.

Mr. J. Reid: If they had the tie-in to the system, yes.

• 1705

Mr. Robinson (Etobicoke—Lakeshore): So how would they go about tying into the system?

Mr. J. Reid: Usually a phone line, or . . .

Mr. Robinson (Etobicoke—Lakeshore): Trial and error?

Mr. J. Reid: —some sort of a telecommunication line.

Mr. Robinson (Etobicoke—Lakeshore): Using the same lines that go into the corporate . . .

Mr. J. Reid: Yes. It would depend on the communication network that the system itself was tied into. If the system itself was totally within the premises, then you could not remote access it. But if there is any remote access to the system, then you are going to be able to connect into the system in the same manner.

Mr. Robinson (Etobicoke—Lakeshore): Well, is there not always a remote access?

Mr. J. Reid: No, not necessarily.

Mr. Kaufman: But there should be no difference, in our view, whether it is inside or outside, where the access is from. It is the question of a commission of the offence that I think is

[Traduction]

de faire les choses actuellement est acceptable. Dans ce cas-ci, il ne s'agirait que d'une infraction comme toutes les autres. Je ne vois pas pourquoi il faudrait aller plus loin.

M. J. Reid: Si vous voulez procéder de cette façon dans le cas de l'abus des systèmes informatisés, vous devez envisager de faire de même ailleurs. Il y a actuellement beaucoup d'escrocs qui ne sont pas signalés par leurs employeurs. Le défaut de signaler une infraction peut être un sujet intéressant, mais il n'existe pas que pour l'abus des systèmes informatiques. Pour ce qui est de la deuxième partie de votre question, vous voulez bien la répéter, s'il vous plaît? Nous ne vous avons pas très bien compris.

M. Robinson (Etobicoke—Lakeshore): A mon avis, il n'y a pas que le vol commis de l'intérieur ou l'abus des systèmes informatiques. Il y a aussi le vol commis de l'extérieur ou l'abus des systèmes informatiques.

M. J. Reid: Vous voulez dire par quelqu'un qui n'est pas un employé? Quelqu'un qui est de l'extérieur.

M. Robinson (Etobicoke—Lakeshore): Oui.

M. J. Reid: Je comprends.

M. Robinson (Etobicoke—Lakeshore): Je suppose qu'il faut d'abord un terminal pour avoir accès à l'ordinateur.

M. J. Reid: Oui.

M. Robinson (Etobicoke—Lakeshore): On peut être n'importe où. De l'autre côté de la rue, dans l'immeuble voisin ou quelque chose du genre.

M. J. Reid: Si on est relié au système, certainement.

M. Robinson (Etobicoke—Lakeshore): Comment ferait-on dans ce cas pour avoir accès au système?

M. J. Reid: On utiliserait une ligne téléphonique ou . . .

M. Robinson (Etobicoke—Lakeshore): On essaierait au hasard?

M. J. Reid: . . . une ligne de télécommunications quelconque.

M. Robinson (Etobicoke—Lakeshore): Il s'agirait de la même ligne qu'utilise la société impliquée . . .

M. J. Reid: Oui. Tout dépendrait du réseau de télécommunications auquel serait relié le système lui-même. Si le système se trouve entièrement dans les locaux de la société, il serait impossible d'y avoir accès de l'extérieur. Cependant, s'il y avait une part du système qui est à l'extérieur, il serait possible de s'y rattacher de la même façon que la société impliquée.

M. Robinson (Etobicoke—Lakeshore): N'y a-t-il pas toujours une partie du système qui est à l'extérieur?

M. J. Reid: Pas nécessairement.

M. Kaufman: Selon nous, il ne devrait pas y avoir de différence, que l'infraction soit commise de l'intérieur ou de l'extérieur. C'est le fait de commettre l'infraction qui est

[Text]

relevant. One could argue that perhaps the access from a third party outside, like a competitor to your information bank, is more serious in consequence to you than an employee playing around with some information, who is inside. That may be true, but it seems to me the misuse of the data is still the same thing, and whether it is done from a thousand miles or right on top of the computer is irrelevant.

Mr. Robinson (Etobicoke—Lakeshore): I think your in-house guidelines and control is something you really have more control over than something from outside, and I was wondering what kind of safeguards you have against, say, your competitor who is down the street.

Mr. Kaufman: Security system. It is the same security system, but if he has the time, effort and the brains, and a phone line, he can access; he can break it eventually. Maybe not; maybe it is sophisticated enough. Maybe if we change it frequently enough, he cannot get into it. But it is possible. The employee you have inside, you equally have no control over, even though you have certain guidelines. If he or she is determined to do something, you are not there watching, and even if you have a security system, it still may break down, particularly if that person is capable of understanding how the whole security system was set up. It is not easy; I do not think it is an easy situation to have to overcome, but it is possible.

Mr. Dean: Locks can be picked and security systems, given the time, can be broken down. This remote situation, though, would find the offsite terminal in a branch office of the owner or the possessor of the computer system; so while it is offsite, it is still really internal. Somebody would have to get on to the system somehow and access it through the computer system that belongs to the possessor of the data bank. If it were a wiretap kind of situation where somebody brought along their own terminal and plugged in between the central processing unit and the remote terminal, accessed the line and got in that way, that brings up a different set of concerns, and one wonders whether the current wiretapping legislation would stop that kind of thing, because you are pulling it off and recording it without either end of the line knowing that was happening.

Mr. Robinson (Etobicoke—Lakeshore): You are saying that this would all have to be done through a wire system.

Mr. Dean: Yes.

Mr. Robinson (Etobicoke—Lakeshore): There is no other way.

The Chairman: Not now.

Mr. Dean: To get at the data . . .

The Chairman: Not now. But we can envisage a time, and maybe not too long, where it could be done, even without wire,

[Translation]

important. On peut toujours faire valoir que l'infraction qui est commise par une tierce partie de l'extérieur, par exemple, par un concurrent qui décide de se relier à votre banque de données, est plus grave que celle qui est commise par un employé qui s'amuse avec l'information. C'est peut-être vrai, mais il y a mauvais usage des données dans un cas comme dans l'autre. Peu importe que l'infraction soit commise à des milliers de milles de distance ou juste à côté de l'ordinateur lui-même.

M. Robinson (Etobicoke—Lakeshore): Vous pouvez quand même avoir un meilleur contrôle sur vos procédés internes que sur ce qui se passe à l'extérieur. Je me demandais seulement quelles garanties vous aviez en place contre les intrusions de votre concurrent qui se trouve dans la même rue que vous, par exemple.

M. Kaufman: Nous avons notre système de sécurité, le même que pour tous les autres. Cependant, si notre concurrent est prêt à y consacrer le temps, les efforts et les connaissances nécessaires, s'il a une ligne téléphonique, il peut parvenir à avoir accès à notre banque. D'autre part, notre système de sécurité peut être suffisamment perfectionné. Si nous y apportons des changements avec une fréquence suffisante, il se peut que nous l'empêchions de procéder. Mais tout reste possible. Pour ce qui est des employés, il est impossible de maintenir un contrôle sur eux, même s'ils sont sujets à certaines directives. Un employé qui y tient absolument peut faire quelque chose. Il est impossible de le surveiller constamment. Il se peut également que le système de sécurité soit en défaut. C'est d'autant plus plausible si l'employé sait comment il fonctionne. Il est impossible de tout prévoir dans ce genre de situation.

M. Dean: Les serrures peuvent être brisées, les systèmes de sécurité neutralisés. Pour revenir à l'accès de l'extérieur, il faut se rappeler qu'il y a des filiales de la société qui sont à l'extérieur et qui peuvent avoir des terminaux. Dans ce cas, il s'agit de terminaux de l'extérieur, mais qui relèvent quand même de la société. Pour commettre une infraction, il faudrait se rattacher au système qui appartient à la société. Si on décidait d'utiliser son propre terminal et de le rattacher à un point quelconque situé entre l'ordinateur central et le terminal à distance, on ferait de l'écoute électronique. La législation existante sur l'écoute électronique serait peut-être suffisante à ce moment-là pour empêcher les gens de procéder. Ce serait équivalent à enregistrer quelque chose, sans que les parties à l'une et l'autre des extrémités de la ligne le sachent.

M. Robinson (Etobicoke—Lakeshore): Il faudrait de toute façon être rattaché à une ligne.

M. Dean: Oui.

M. Robinson (Etobicoke—Lakeshore): Il n'y aurait pas d'autres façons de procéder.

Le président: Pas pour l'instant.

M. Dean: Pour avoir accès à l'information . . .

Le président: Il n'est pas dit, cependant, qu'un jour on ne pourra pas procéder autrement, au moyen d'un récepteur, par

[Texte]

just a transmitter, like the radio waves or any other means of contacting a computer to other mechanisms other than using a telephone or a telecommunications line.

Mr. J. Reid: I was just going to say, right now it is electronic transmission, and if we go to some other form of transmission, then it is going to be another way of accessing, but right now electronic transmission is the way we do it.

Mr. Dean: If the data is supersensitive, in the opinion of the owner of the data, it would behave them not to have a computer system that had the remote kind of access. Just as in the military, when lines are insecure, you do not use lines; you use dispatch runners. You can have centralized systems and then transport the data physically and avoid the problem, if that is your choice because of the degree of security you want. But then again it is up to the holder to make those decisions.

• 1710

The Chairman: And we all go back to the authorized and unauthorized information. Some information might create no damage whatsoever, and anybody who wants to have access could have access; and on the other hand, the unauthorized access, well this is the one that has some value and that we should tackle in our report.

Anyway, I would like to thank you for joining us this afternoon and for sharing your views and knowledge. Certainly, we will take into consideration what you have prepared for us. Since we are not going to report next week, if you have other information to put forward after coming to this committee, we would be pleased to receive any other suggestions.

Mr. Robinson (Etobicoke—Lakeshore): Just before we adjourn, Madam Chairman, I wonder if they might be able to provide us with—not really their sales pitch—some of the information they use by way of selling the computer system. The brochures or the dialogue that is used would be very helpful, I think, to the committee.

Mr. J. Reid: I think we could put together something that will show you how the security issue is addressed.

Mr. Dean: Sure.

The Chairman: Okay, I think we would like that. Thank you so much.

Merci, monsieur Robinson.

La séance est levée.

[Traduction]

exemple, pouvant capter les ondes comme les ondes radiophoniques, ou autrement. Il se peut qu'on ne soit pas obligé un jour de passer par les lignes téléphoniques ou les lignes de télécommunication.

M. J. Reid: Nous utilisons actuellement un mode de transmission électronique. Si jamais nous adoptons un autre mode de transmission, il est certain qu'il existera d'autres moyens de se rattacher au système.

M. Dean: Si le propriétaire de l'information estime cette information de nature très délicate, il évite évidemment d'avoir un système accessible de l'extérieur. Chez les militaires, par exemple, lorsque les lignes de communication ne sont pas sûres, on ne les utilise pas. On a recours à des porteurs de dépêches. Rien n'empêche quelqu'un de faire transporter son information par des personnes. Tout dépend du degré de sécurité qu'il souhaite avoir. Je le répète, ce genre de décision doit appartenir au propriétaire de l'information.

Le président: Nous voilà revenus à la question de l'information autorisée et non autorisée. Il y a de l'information qui ne risque pas de faire de tort à qui que ce soit et qui est disponible à quiconque désire l'obtenir. Il y a également de l'information qu'on n'est pas autorisée de recevoir. Nous devons en tenir compte dans notre rapport.

Je vous remercie d'avoir bien voulu vous joindre à nous cet après-midi et de nous avoir fait part de vos vues et de vos connaissances. Nous examinerons sûrement la documentation que vous nous avez soumise. Cependant, nous ne préparerons pas notre rapport la semaine prochaine. Si vous avez un supplément d'information à nous donner après votre passage ici, n'hésitez pas à communiquer de nouveau avec nous.

M. Robinson (Etobicoke—Lakeshore): Avant que vous ne mettiez fin à la réunion, madame le président, je voudrais savoir si les témoins sont prêts à nous remettre non pas leurs arguments de ventes mais l'information qu'ils communiquent aux clients qui achètent leur système. Les brochures qu'ils utilisent, les instructions qu'ils donnent pourraient être utiles au Comité.

M. J. Reid: Nous pouvons vous remettre des dépliants qui vous indiqueront que nous nous intéressons à la question de la sécurité.

M. Dean: Certainement.

Le président: Nous vous en serions reconnaissants. Merci.

Thank you, Mr. Robinson.

The meeting is adjourned.



If undelivered, return COVER ONLY to
Canadian Government Printing Office
Supply and Services Canada
45 Sacre-Coeur Boulevard
Hull, Quebec, Canada, K1A 0S7

En cas de non-livraison
retourner cette COUVERTURE SEULEMENT à
Imprimerie du gouvernement canadien
Approvisionnement et Services Canada
45 boulevard Sacre-Coeur
Hull, Quebec, Canada, K1A 0S7

WITNESSES—TÉMOINS

From the Canadian Business Equipment Manufacturers Association:

Mr. John Reid, Chairman of the Legislation Committee (CBEMA);
Mr. Howard Kaufman, Vice-President of Xerox;
Mr. John Dean, Senior Legal Advisor of IBM.

De l'Association canadienne des fabricants d'équipement de bureau:

Mr. John Reid, Président du Comité de législation (ACFEB);
M. Howard Kaufman, Vice-président de Xérox;
M. John Dean, Conseiller juridique sénior de IBM.

HOUSE OF COMMONS

Issue No. 4

Wednesday, April 27, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 4

Le mercredi 27 avril 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

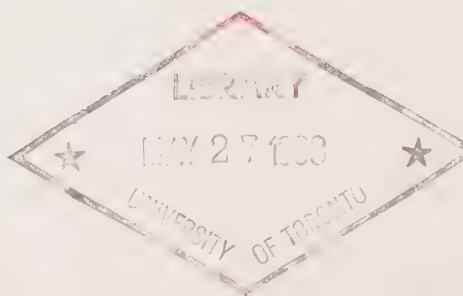
Questions relatives à l'Ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, APRIL 27, 1983

(6)

[Text]

The Sub-committee on computer crime met this day at 3:40 o'clock p.m. the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Céline Hervieux-Payette.

Designate alternates Members present: Mr. Beatty and Mr. Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witness: From Peat, Marwick and Partners: Mr. Peter Ward, Toronto.

The Sub-committee on computer crime resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings of Tuesday, March 15, 1983, Issue No. 1*).

Mr. Ward made a statement and answered questions.

At 4:46 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 27 AVRIL 1983

(6)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h.40 sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Céline Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présents: M^{me} M. Hébert, Recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoin: De «Peat, Marwick and Partners»: M. Peter Ward, Toronto.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1*).

M. Ward fait une déclaration et répond aux questions.

A 16h46, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Wednesday, April 27, 1983

• 1540

Le président: La séance est ouverte.

Cet après-midi, le Sous-comité sur les infractions relatives aux ordinateurs du Comité permanent de la justice et des questions juridiques accueille M. Peter Ward de *Peat, Marwick and Partners*, de Toronto. J'invite le témoin à faire sa déclaration et nous procéderons ensuite à une période de questions.

Bienvenue, monsieur Ward.

Mr. Peter Ward (Peat, Marwick and Partners, Toronto): Thank you, Madam Chairman, Mr. Beatty. On behalf of the partners at Peat, Marwick perhaps I can thank you for the opportunity of being here to present what I consider some very important thoughts on this issue.

I must say that I hope this brief commentary . . . and I will try and keep it brief, which is unusual with management consultants . . . and answering any questions you may have, will really provide you with some insight.

I think my comments today really relate to the practical perspective on computer crime. I am aware that you have talked to many people who have an interest, but my interest is very much from a practical perspective as a management consultant, really as a partner in charge of a significant group of professionals involved in providing computer consulting services to clients in both the private and public sectors. I am involved with computer systems from the micro-computer in small businesses right through to the large computer systems, national computer networks used by our large chartered banks.

I should add that my own area of specialization, really since 1969, has been the use of computers in banking. So I am very keenly aware of the potential that exists for the misuse of computers when there are some very significant sums of money involved.

As I was preparing my notes, it was interesting to reflect back over the last 10 years, since I joined Peat, Marwick, and to note that I have been involved in only one client situation which could be even remotely considered as computer crime, as I believe has been defined to you over the past several weeks. Really, all this was was the illegal access to data in a Toronto-based computer from the San Francisco Bay area by what I believe is called in the trade somebody who was joy-riding. Again, no damage to the data, no damage to the company, and it was not possible to identify or apprehend the perpetrator in this situation. As the saying goes, the stable door was certainly closed in that case after the horse had bolted, and we were involved, if you like, in closing that stable door. But it was a very real situation, but the only one, may I

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mercredi 27 avril 1983

The Chairman: Order, please.

This afternoon we, as the Subcommittee on Computer Crime of the Standing Committee on Justice and Legal Affairs, welcome Mr. Peter Ward from Peat, Marwick and Partners of Toronto. I will ask the witness to present his opening statement, after which we will have our question period.

Welcome to you, Mr. Ward.

M. Peter Ward (Peat, Marwick and Partners, Toronto): Merci, madame le président, et merci à vous aussi, monsieur Beatty. Au nom de la maison Peat and Marwick, j'aimerais vous remercier de cette occasion que vous me donnez aujourd'hui de vous faire part de certaines idées que je juge très importantes à propos de ce dossier.

Je dois dire que j'espère que ce bref commentaire—car telle est mon intention, ce qui est un peu inhabituel pour un expert-conseils en matière de gestion—et mes réponses à vos questions vous donneront une perspective utile.

Ce que j'ai à vous dire aujourd'hui porte davantage sur le crime informatique vu sous l'angle pratique. Je sais que vous avez déjà rencontré bien des gens qui s'intéressaient à ce problème, mais en ce qui me concerne, je suis surtout attiré par l'angle pratique de la question puisque je suis expert-conseils en matière de gestion et, plus précisément, que je m'occupe pour ma firme d'un imposant groupe de spécialistes appelés à fournir à nos clients des secteurs public comme privé des services-conseils en matière informatique. Je travaille dans le domaine des systèmes informatiques, ce qui va des micro-ordinateurs utilisés par la petite entreprise jusqu'aux mégaréseaux informatiques nationaux dont se servent nos grandes banques à charte.

Je dois également ajouter que, depuis 1969, je me spécialise dans l'utilisation des ordinateurs à des fins bancaires et je suis d'ailleurs parfaitement au courant des possibilités omniprésentes d'utilisation abusive des ordinateurs, ce qui sous-tendrait des sommes extrêmement importantes.

En préparant mon exposé, j'ai fait un retour en arrière d'une dizaine d'années, jusqu'à l'époque où j'ai commencé à travailler pour Peat et Marwick, et en y réfléchissant, je me suis rendu compte que, pendant toute cette période, je n'avais eu connaissance directe que d'un seul cas de client ayant été la victime de ce qu'on pourrait considérer d'une façon extrêmement indirecte comme un crime informatique, selon la définition qui, je crois, vous a été donnée il y a quelques semaines. En fait, il s'agissait simplement de l'utilisation illicite de la mémoire informatique d'un ordinateur situé à Toronto, utilisation faite depuis la région de la Baie de San Francisco par quelqu'un qu'on appelle, je crois, dans le jargon du métier un petit resquilleur. Je m'empresse d'ajouter que la mémoire n'a pas été endommagée, que la compagnie n'a subi

[Texte]

add, in 10 years and probably hundreds of clients where I actually came across computer crime.

Prior to starting my remarks I think I would like to just comment on the presentation made to you by Superintendent Allen of the RCMP⁴ I believe it really represents an excellent summary of the issues that must be addressed in computer crime.

I think the recommendations are both practical and realistic in light of what I would suggest is the potential magnitude of the problem. Again, I will not attempt to repeat the types of discussion that Superintendent Allen contained in his paper, and for that reason.

Having said that, may I now turn onto one of our significant concerns in the area of computer crime. Really, that is the issue of separating what is myth from reality. In the area of computer crime, and I am sure you have all heard it over the past several weeks, I firmly believe we are in danger of reinventing Greek mythology in modern times.

What has been written on computer crimes and spoken about it? These are just a few of the quotes, and I am sure that you in the committee have many, many more quotes provided to you from the documentation. One from *Canadian Business* which in 1979 said that it is estimated that \$300 million is lost world-wide each year through computer abuse.

• 1545

A second, from *Management Accounting*, in April 1978, said that the loss from computer abuse will probably go past \$1 billion . . . I cannot even think how many zeros there are in \$1 billion—but \$1 billion by 1980.

One of the favourite quotes in computer crime is that over 85% of computer crime goes unreported. Last time I heard that it was the Solicitor General of Ontario, sitting next to me at an Ontario provincial police computer crime seminar, who provided that information.

I think these are just three comments from what we believe is the mythology that surrounds computer crime. I think as in Greek mythology we should also go back to the source to find out where they came from. I will pick the last one, and read a paragraph from a letter by Mr. Donn Parker. I believe Mr. Parker's name is probably contained in a lot of the literature you have read.

[Traduction]

aucun préjudice, mais également qu'il n'a pas été possible d'identifier ni d'appréhender le coupable. Comme dit le proverbe, nous avons en fait fermé la porte de l'écurie après que le cheval se soit échappé, et d'une certaine façon, c'est nous qui avons fermé la porte de cette écurie. Il n'empêche que la situation s'est produite mais, même là, je dois répéter que c'est le seul dossier dont j'ai eu connaissance en dix ans et sur une clientèle totale de plusieurs centaines d'entreprises.

Avant de commencer, je devrais dire quelques mots à propos de l'exposé du surintendant Allen de la GRC qui a, je crois, parfaitement résumé les problèmes sur lesquels il faut se pencher en matière de crime informatique.

Les recommandations de M. Allen sont à mes yeux à la fois commodes et conformes à la réalité, compte tenu de l'envergure possible du problème tel que je l'envisage. Ici encore, je ne tiens pas à répéter les arguments du surintendant Allen pour cette même raison.

Cela dit, j'aimerais vous faire part des problèmes importants que nous percevons en matière de crime informatique. En réalité, il importe avant tout, c'est le problème principal, de faire la distinction entre le mythe et la réalité. En parlant de crime informatique, et je suis sûr que vous en avez entendu parler à maintes reprises depuis quelques semaines, je suis fermement convaincu que nous risquons de réinventer une nouvelle mythologie classique.

Qu'a-t-on dit et écrit à propos du crime informatique? Je vais vous lire quelques citations et je ne doute pas que vous en ayez entendu ou lu bien d'autres depuis le début de vos travaux. En premier lieu, la revue «*Canadian Business*» affirmait en 1979 que l'utilisation abusive des ordinateurs à l'échelle mondiale coûtait chaque année, selon ses calculs, 300 millions de dollars.

Une seconde citation, extraite celle-là de la revue *Management Accounting* du mois d'avril 1978, prétendait que l'utilisation abusive des ordinateurs allait probablement, en 1980, coûter plus d'un milliard de dollars—chiffre dont je ne parviens même pas à me représenter le nombre de zéros.

L'une des citations que j'affectionne le plus à propos du crime informatique est celle qui dit que plus de 85 p. 100 des actes criminels en matière informatique ne sont jamais signalés. La dernière fois que je l'ai entendue, c'était à l'occasion d'un colloque organisé par la Police provinciale de l'Ontario à propos du crime informatique, colloque auquel j'ai assisté avec, pour voisin immédiat, le Solliciteur-général de cette province.

Voilà donc trois extraits qui renforcent ma conviction selon laquelle le crime informatique est devenu une véritable mythologie. Comme dans le cas de la mythologie classique, nous devrions nous attacher à remonter aux sources pour vérifier l'origine. Prenons la dernière citation. Je vais vous lire un extrait d'une lettre de M. Don Parker dont le nom, j'imagine, revient souvent dans les documents que vous avez lus.

[Text]

In my book, *Crime by Computer*, I explain the 85% figure...

—and I think if you follow back, by the way, that 85% figure, you always find Mr. Parker is the source of origin...

... based on a study of reported violent crime in Detroit. A more recent study in Los Angeles showed the same. I have reasoned that probably fewer white collar crimes than violent crimes are reported. Therefore, it is likely that more than 85% of computer crimes go unreported.

Having said that, while not being expert on violent crime, I have to say it is difficult for us to understand how a correlation can be drawn so closely between the two. I suggest if Mr. Parker's contention is correct, it appears we have a large number of negligent senior managers in both our private and our public sector organizations who refuse to report to the appropriate authorities that crime has taken place—a very disturbing situation, if that is the case.

The reality of the situation as contained in available published information is somewhat different. Certainly I am aware Mr. Beatty has a copy of an article written by one of my managers in the *CA Magazine* of January 1981, and I believe it should be reading material for the committee, concerning computer crime, with some information; and much of the information I am going to discuss now is taken from that article.

These are verifiable facts: that approximately 75 reported worldwide cases of computer abuse have occurred each year. I would like to stress the one word "reported" in that. The number of reported cases appears to be levelling off. In fact, if you look at charts in Mr. Parker's books recently, and in some material produced by the Stanford Research Institute, the earlier predictions from the mid-1970s of phenomenal growth in computer crime were not met during the late 1970s. The same information shows that the average annual reported loss is approximately \$40 million, again on a worldwide basis. And finally, another fact is that the Ontario Provincial Police, Inspector Campbell, of the Anti-Rackets Branch, conducted a survey, I believe just over a year or 18 months ago, when in fact only 2% of the surveyed companies reported any instance whatever, in a very broad definition of computer crime.

Moving on, while such facts do not fully disprove the myths which have arisen, I believe they do raise sufficient questions in the mind of a practical professional, such as myself, to suggest that some further research and study of the problem is required. We would suggest that a major information gap

[Translation]

Dans mon ouvrage intitulé *Crime by Computer*, j'explique ce chiffre de 85 p. 100...

—et, entre parenthèses, si vous essayez de retrouver l'origine de ce chiffre de 85 p. 100, vous tombez inmanquablement sur le nom de M. Parker

... en disant qu'il était fondé sur une étude des actes criminels accompagnés de violence signalés à Détroit. Une étude plus récente encore effectuée à Los Angeles arrive à la même conclusion. J'en ai conclu que les cas d'actes criminels perpétrés au niveau des employés de bureau devaient être encore moins nombreux à être signalés. Il est dès lors très vraisemblable que plus de 85 p. 100 des crimes informatiques soient passés sous silence.

Cela dit, même si je ne suis nullement expert en matière de crimes accompagnés de violence, je dois pourtant préciser qu'il nous est très difficile de comprendre comment on peut faire un parallèle aussi rigoureux entre les deux. Selon moi, si M. Parker a raison, il y aurait selon toute apparence énormément de cadres supérieurs très négligents tant dans le secteur privé que dans le secteur public, négligents dans la mesure où ils refuseraient de signaler aux autorités compétentes les actes criminels qui se seraient produits, une situation assez inquiétante, dirais-je, si c'était effectivement le cas.

Mais la réalité, comme en font état de nombreux documents, est quelque peu différente. Je sais que M. Beatty a une copie d'un article rédigé par un de mes administrateurs dans le numéro de janvier de 1981 de la revue *CA Magazine*, et qu'il me soit permis de vous dire qu'il s'agit d'une excellente documentation de référence sur le crime informatique pour le Comité. Cet article contient une masse de renseignements et le plus clair de ce dont je vais vous parler maintenant provient de cet article.

Voici des chiffres vérifiables: à l'échelle mondiale, on signale chaque année environ 75 cas d'utilisation abusive des ordinateurs, j'aimerais d'ailleurs insister sur le terme «signaler». Le nombre de cas ainsi signalés semble également plafonner. Si vous vous reportez aux tableaux publiés tout récemment dans les ouvrages de M. Parker et à ceux qui contiennent les documents publiés par le *Stanford Research Institute*, les premières prévisions qui remontaient au milieu des années '70 et qui faisaient état d'une croissance absolument phénoménale du crime informatique ne se sont jamais matérialisées à la fin des années '70. Ces mêmes données nous montrent que les pertes annuelles moyennes signalées se chiffrent à environ 40 millions de dollars, et il s'agit une fois encore de chiffres valant pour le monde entier. Enfin, l'inspecteur Campbell, de la Division des escroqueries de la Police provinciale de l'Ontario, a procédé il y a un peu plus d'un an, peut-être dix-huit mois, je crois, à une enquête qui lui a permis de conclure que sur toutes les compagnies interrogées, 2 p. 100 seulement avaient signalé des cas de ce genre, et encore s'agissait-il d'une définition extrêmement générale du crime informatique.

Dans la même veine, même si tous ces faits et ces chiffres ne permettent pas de dissiper les mythes qui sont nés, ils permettent quand même, dirais-je, aux spécialistes de la profession comme moi de conclure que cette question exige un sérieux complément de recherches et d'analyses. Selon nous, il existe

[Texte]

exists in Canada as to the extent and nature of computer crime. I am digressing slightly, but one suggestion for the subcommittee to consider is that the federal government should sponsor a research study, possibly with the universities, aimed at quantifying in absolute terms the nature and extent of computer crime. There is no reason why such a study could not run in parallel with other initiatives aimed at strengthening legislation. It would really provide a more factual base than you have to work from today on which to develop the preventive programs which must be put in place to minimize our risk.

That sort of suggestion is not taken lightly, because it is very difficult for the police departments, for organizations, really to know what investment to make in this area. Until we have some facts, it is very difficult to decide the level of investment. I would suggest if we are using the so-called "facts" that are bandied around in this area, one should be very careful where these "facts" come from.

• 1550

Having said that—and really that is the major point I wish to make today—I must hasten to add that we are not saying that computer crime is not a major problem. I suggest that the situation is that nobody really knows if a problem exists. I have heard speculation from some very senior people in the field that the increased awareness of the potential for computer crime, both by businesses, government and the law enforcement communities, really has led us to a situation where the increased diligence from publicity has resulted in improved controls which effectively have lowered the rate of computer crime. However, we should remember that the potential does exist, as more and more of our lives are becoming computerized, if I could use that word, for a major computer fraud.

Two areas where significant benefit could be gained by the criminal should a major computer crime be perpetrated are in our financial institutions and the federal government. In both cases the computers really are playing an increasing role in the management and operation of the organization. Think of the banks for a second: the millions of dollars of depositors' funds in that case, or the critical and confidential information in the federal government's case, could easily be stolen if that were the case. But again, in my own work with the banks and with the federal government in working here for seven years, both organizations are really putting a lot more emphasis on computer security.

[Traduction]

actuellement au Canada un énorme fossé dans nos connaissances de l'envergure et de la nature du crime informatique. Je fais ici une légère digression, mais le Sous-comité pourrait utilement envisager la possibilité que le gouvernement fédéral commandite un projet de recherche, qui pourrait peut-être être exécuté conjointement avec les universités et qui aurait pour but de chiffrer d'une façon absolue l'envergure et la nature du crime informatique. Cette étude pourrait parfaitement se dérouler parallèlement à d'autres initiatives axées par exemple sur un resserrement de la législation actuelle. Elle permettrait en plus d'obtenir un ensemble de données parfaitement étayées et beaucoup plus valables que celles sur lesquelles vous devez vous baser aujourd'hui pour mettre au point les programmes à caractère préventif qui s'imposent si nous voulons réduire les risques au minimum.

Voilà une proposition à ne pas prendre à la légère car il est, à l'heure actuelle, extrêmement difficile aux corps policiers et aux organismes de déterminer au juste ce qu'il importe d'investir dans ce domaine. Tant que nous n'aurons pas de données solides, il sera très difficile de décider d'un seuil d'investissements. Je dois ajouter que si nous devons utiliser ces «faits» comme on les appelle actuellement et qui portent sur l'ensemble de ce domaine, il ne faut le faire qu'avec beaucoup de prudence en sachant pertinemment quelle est leur source.

Cela dit, et c'est en fait la principale chose que je voulais vous signaler aujourd'hui, je m'empresse d'ajouter que nous ne voulons nullement prétendre que le crime informatique n'est pas un problème d'envergure. La situation vous dirais-je est qu'en fait, personne ne sait au juste s'il y a effectivement un problème. J'ai entendu certains spécialistes très éminents avancer l'hypothèse qu'une sensibilisation accrue aux risques possibles de crimes informatiques de la part tant des milieux d'affaires, ou gouvernementaux et policiers, nous a en fait amené à un état de choses tel que la multiplication des initiatives découlant directement de toute cette publicité s'est traduite par un resserrement des mesures de contrôle, avec pour conséquence pratique une diminution du nombre de crimes informatiques. Nous ne devons toutefois pas oublier que les possibilités restent entières dans la mesure où nos vies deviennent de plus en plus informatisées, si vous me passez le terme, possibilités ouvrant directement sur des fraudes de grande envergure rendues possibles par l'ordinateur.

L'éventualité d'un crime informatique d'envergure pourrait frapper tout particulièrement nos institutions financières et le gouvernement fédéral car, dans les deux cas, les ordinateurs jouent un rôle de plus en plus important au niveau des activités de gestion et d'exploitation. Pensez un instant aux banques où des millions de dollars sont en dépôt, pensez également aux renseignements confidentiels et extrêmement importants que conserve le gouvernement fédéral. Quoi de plus facile que d'aller les voler en utilisant l'ordinateur? Une fois encore pourtant, je dois vous dire qu'à force de fréquenter depuis sept ans les banques et le gouvernement fédéral, je me suis rendu compte que les unes comme le second insistent de plus en plus sur les mesures de sécurité informatique.

[Text]

I may just add a few comments here that that emphasis is not being placed solely for the reasons of preventing computer crime. This emphasis is placed to stop misuse, abuse, whether that be intentional or otherwise, of the computer. In fact, most of the controls that are being put in place, very expensive controls in computer systems, are really to stop the accidental disclosure of information, accidental corruption of information, as opposed to intentional, fraudulent changes to information.

Madam Chairman, members of the subcommittee, I hope that these brief remarks will provide you with food for thought in this area, and perhaps I can turn the floor over to you and answer any questions that you may have at this time.

The Chairman: Thank you.

Monsieur Beatty, avez-vous des questions?

Mr. Beatty: Thank you, Madam Chairman. Mr. Ward, thank you for your presentation, which helps to put the issue in some perspective. I guess the obvious question that comes to mind is: Do you feel there is a need at present for new legislation?

Mr. Ward: I refer back to Superintendent Allen's paper. Again, that talks about the need for legislation. There is certainly need for legislation where the computer is the object of the crime; i.e., the illegal access to data. Again, a lot of that type of illegal access is probably not reported in that (a) it may never be seen and (b) the situation I described right at the beginning of my remarks does not cause any damage because it is the joy-riding. But, again, I believe in Superintendent Allen's presentation he does make reference to the need for legislation to dissuade the potential criminal, and certainly we would strongly support, as does, I believe, Superintendent Allen, the need for legislation in the area where the computer is the object of the crime.

Mr. Beatty: What specifics would you recommend?

Mr. Ward: I think we have somewhat of a problem in here in that there is need for legislation but the type of legislation that one might want to put in place would be so complex... With all due respect to the decision-makers and all due respect to the people who make the legislation, it would be terribly complex from a technical perspective to have ironclad legislation in this area.

I think what we need is a degree of legislation that will deter the would-be joy-rider, would deter the person who is attempting to gain access to that information, which is relatively easy to interpret and to enforce. I think we have seen in the past examples of legislation in this general area which are very difficult to enforce because of the changing technology with which we are faced.

[Translation]

J'aimerais ajouter deux ou trois éléments pour vous signaler que cette insistance n'a pas exclusivement pour but d'empêcher les crimes informatiques. Il s'agit surtout de mettre un frein aux utilisations abusives, intentionnelles ou non, dont les ordinateurs font l'objet. De fait, la majeure partie des mesures de contrôle qui sont implantées à très grands frais dans les systèmes informatiques ont effectivement pour but d'enrayer le nombre de cas de divulgation ou de déformation accidentelle des données, par opposition à la manipulation frauduleuse et intentionnelle de ces mêmes données.

Madame le président, messieurs les membres du Sous-comité, j'espère que ces quelques mots vous auront donné matière à réflexion. Peut-être pourrais-je maintenant vous rendre la parole et répondre à vos questions.

Le président: Je vous remercie.

Mr. Beatty, any questions?

M. Beatty: Merci, madame le président. Je vous remercie pour votre exposé, monsieur Ward, car il nous aura aidés à mettre le problème dans son contexte. J'imagine que la première question qui nous vient à l'esprit est la suivante: pensez-vous qu'à l'heure actuelle une intervention législative s'impose?

M. Ward: Je vous renvoie à ce sujet à ce que disait le surintendant Allen dans son exposé où il parlait effectivement de la nécessité d'une intervention législative. Il est évident que la législation doit pouvoir couvrir les cas où l'ordinateur est la victime en quelque sorte de l'acte criminel, et je pense par exemple à l'utilisation illicite des données. Mais ici encore, il est probable qu'énormément de cas d'utilisation illicite ne soient pas signalés, en premier lieu parce qu'ils peuvent fort bien passer inaperçus et en second lieu parce que, lorsqu'il s'agit d'un simple resquillage, aucun tort n'est causé comme je le disais au début de mon intervention. Il n'empêche que M. Allen parlait effectivement dans son exposé de la nécessité d'une intervention législative, ne serait-ce que pour dissuader les éventuels criminels, et à cet égard, je serais tout à fait favorable, comme j'imagine le surintendant Allen, à une intervention législative pour les cas d'actes criminels dont l'ordinateur serait la victime.

M. Beatty: Que recommanderiez-vous plus précisément?

M. Ward: J'imagine qu'en l'occurrence, le problème, c'est qu'effectivement nous avons besoin d'une intervention législative, mais que la loi qu'on voudrait peut-être voir adoptée serait extrêmement complexe... Je ne veux nullement manquer de respect à l'endroit des décideurs et des législateurs, mais il faut bien avouer que d'un point de vue technique, une mesure législative en béton armé serait dans ce domaine extraordinairement complexe.

Il nous faudrait, dirais-je, une mesure législative susceptible de dissuader le petit resquilleur, de dissuader quiconque envisagerait d'aller à la pêche illicite aux données, une mesure législative qui serait également facile à interpréter et à faire respecter. Dans ce domaine général, nous avons déjà eu des mesures législatives de ce genre qui se sont révélées extrêmement difficiles à mettre en oeuvre en raison de l'évolution constante de la technologie.

[Texte]

I would suggest that it would be difficult at this point in time to guess in five years what some of the technological challenges would be in preparing the legislation today. In the whole thing of micro-computers, for example, five years ago one would not have foreseen, possibly, their use today and in five more years' time we might see many other things that we are not really too, too aware of today. So in putting the legislation together, my suggestion would be legislation that is relatively simple in its conception, relatively simple in its language, from both the understanding and the implementation of such legislation and really that does not attempt to try to quantify the stealing of the information, I think.

• 1555

To try to quantify the stealing of information from a computer is probably going to be one of the most difficult things for this committee to come to grips with, because a general perception of stealing, certainly in the western world, is to take something physically away from somebody. There are very few examples, there are some but very few, where by not taking anything away from somebody... i.e., you leave everything intact—an offence is committed. That is where the trouble will really be, where somebody has stolen from a visual display screen or had a second copy printed up on a computer—for example, somebody's mailing address list, whose use then makes the company it was stolen from less competitive.

Mr. Beatty: Would it be your suggestion that the simplest way to deal with it would be dealing with theft of service?

Mr. Ward: I think the simplest way might be to deal with illegal access, or unauthorized access, in the first place, i.e. getting into the computer, in laymen's terms, as opposed to taking things out. In every computer installation, more and more so, there are only certain people who are allowed to use that computer: it is a commercial service bureau, it is people who have accounts, who have signed contracts with the supplier of service. If it is a private sector or public sector organization, it is a certain sub set of the employees of that organization who have that access. Maybe to have anybody else accessing it, initially, would be one example of how...

Mr. Beatty: You would have to make it analogous to computer trespassing.

Mr. Ward: Yes, that is correct.

Mr. Beatty: Would this include where you had time-sharing on a main frame and where you are authorized to get into your element of the data base but not into another, but straying from your own area of the data base into somebody else's area would constitute computerized trespass, if you like?

[Traduction]

J'ajouterais que pour l'instant il est assez difficile de deviner ou d'imaginer ce que l'élaboration de cette mesure législative pourrait réserver d'ici cinq ans comme casse-tête technologique. Ainsi, dans le vaste domaine de la micro-informatique, on n'aurait jamais pu prévoir il y a cinq ans les utilisations que nous en faisons aujourd'hui et il se peut fort bien que dans cinq ans, nous assistions à des choses que nous pourrions difficilement concevoir aujourd'hui. Dès lors, lorsqu'il s'agit d'élaborer une mesure législative, je préconiserais une loi relativement simple tant du point de vue de la conception que du point de vue de son libellé, simple à comprendre et à mettre en place, en bref une loi qui n'essaierait pas de chiffrer en quelque sorte le vol des données. Voilà mon avis.

La quantification pratique du vol de données dans une mémoire informatique va probablement être l'une des tâches les plus ardues du Comité, ne serait-ce que parce que, dans le monde occidental du moins, l'acte de voler est perçu comme quelque chose d'essentiellement matériel. Les exemples sont très rares, il y en a quelques-uns mais ils sont très rares, exemples d'infractions qui ne découlent pas du prélèvement matériel de quelque chose de concret au détriment de quelqu'un. Et c'est là justement que le problème va se poser: supposons que quelqu'un veuille un renseignement affiché sur un écran ou fasse imprimer une deuxième copie d'une liste informatique, une liste d'adresses par exemple, avec pour résultat que l'entreprise à qui cette liste appartient verrait sa position concurrentielle s'affaiblir.

M. Beatty: Iriez-vous jusqu'à dire que la façon la plus simple de s'en sortir serait de parler d'un vol de service?

M. Ward: Je pense que la façon la plus simple serait de parler d'utilisations illicites ou d'utilisations non autorisées pour commencer, et j'entends par là le fait de se brancher sur l'ordinateur, pour utiliser une expression de profane, par opposition au fait d'en retirer quelque chose. Il est de plus en plus fréquent, dans tout le système informatique, que seules certaines personnes soient autorisées à se servir de l'ordinateur: dans un bureau spécialisé dans les services commerciaux par exemple, les gens qui détiennent des comptes ou qui ont signé un contrat avec un fournisseur peuvent utiliser l'ordinateur. Dans le secteur privé ou dans le secteur public, un certain nombre d'employés peuvent effectivement se servir de l'ordinateur. Peut-être qu'au départ, on pourrait utiliser l'exemple de l'utilisation de l'ordinateur par quelqu'un d'autre qui n'aurait pas été préalablement autorisé à le faire...

M. Beatty: En fait, on pourrait en faire une analogie avec un genre de violation d'un ordinateur.

M. Ward: C'est bien cela.

M. Beatty: Est-ce que cela vaudrait également dans le cas d'une utilisation partagée d'un ordinateur commun, une personne étant par exemple autorisée à utiliser un certain segment de la mémoire mais non pas un autre? À ce moment-là, la personne qui outrepasserait ses limites et utiliserait le segment mémoriel de quelqu'un d'autre se rendrait effectivement coupable d'une violation d'ordinateur. Est-ce bien de cela qu'il s'agit?

[Text]

Mr. Ward: Certainly. It is relatively easy, even in technical terms, to identify areas of a computer that a person has access to—his or her own data, for example. A particular region—to use a somewhat technical term—of the computer memory is allocated to you as the user, and that can easily be covered on a contractual basis, as it normally is when one enters into a contract for services on a time-sharing basis. So if you, or someone else, goes outside of those boundaries, maybe a crime has been committed at that point.

Mr. Beatty: It is obvious that the easiest way of dealing with this would be on the basis of trespass, if you like, or unauthorized access. But one of the other difficulties, I think, that legislators have is trying to fit the penalty to the crime. Surely, in your own mind, you would be more concerned . . . If you had a Radio Shack pocket computer in your pocket and left it there and I borrowed it and balanced my cheque book with it, it would surely seem to you, as well as to me, to be less an offence than if I were to gain access to a main frame and damage the data base in some way—say from a bank, as you say, where there is the potential of doing very serious damage to individuals and corporations. How would you differentiate between these two different types of crimes in terms of severity when you have one offence, which would be unauthorized access?

Mr. Ward: Again, a very difficult question to answer. When one considers trespass, I am sure there are certain places in Ottawa where if one trespassed one would be in more trouble than in others, with all due respect—say National Defence, or the RCMP. Again, a critical question, there is no easy answer to that. We just thought of the entry to the computer as trespass; maybe one should move on and think about what one does when one is inside as the next level of crime. I think you are quite right, Mr. Beatty, the ability to differentiate what one's intent is—I think that is what you are getting at, if I am correct, one's intent in getting into the computer . . .

Mr. Beatty: Not necessarily. Even if it were a case of joy-riding, I would consider it more serious if the data base were damaged and put a company out of business than if it were simply unauthorized use of time.

Mr. Ward: What I was going to go on to say was, if one considers the access as the first stage, the second stage is what one does when one is in there. Take the example of my client, to whom I referred earlier: there was no apparent damage to the data. This is the next question, I think, that should be

[Translation]

M. Ward: Tout à fait. Techniquement parlant, il est relativement facile de repérer les segments du réseau informatique auxquels quelqu'un peut avoir accès, par exemple le segment de la mémoire qui contient les données qui lui appartiennent. Une région—c'est un terme d'informatique—de la mémoire est attribuée à l'utilisateur, par contrat par exemple, et c'est ce qui se passe normalement pour les contrats de services prévoyant le partage du temps d'ordinateur. Si l'utilisateur outrepassé les limites qui lui sont imparties, il se peut qu'il y ait à ce moment-là crime.

M. Beatty: Il est donc évident que la façon la plus facile d'aborder le problème serait de partir de la notion de violation ou, si vous préférez, d'utilisation non autorisée. Mais j'ajouterais que les législateurs ont d'autres problèmes, et notamment lorsqu'il s'agit de faire correspondre le crime et la peine. Il est certain qu'à votre point de vue, vous seriez plus inquiet . . . Il est certain que si vous oubliez sur la table, votre petite calculatrice de poche Radio Shack et si je vous l'emprunte pour mettre de l'ordre dans mes comptes bancaires, ce serait à vos yeux comme aux miens une infraction bien moins grave, pourrait-on même parler d'infraction, que si je me branchais sur une centrale et que j'en endommageais la mémoire, par exemple la mémoire d'une banque, puisque comme vous le disiez, un acte de ce genre pourrait se révéler extrêmement préjudiciable tant pour les personnes que pour les entreprises. Quelle différence feriez-vous entre ces deux catégories de crime lorsqu'il s'agirait de les punir, et nous parlons ici d'utilisations non autorisées?

M. Ward: Encore une fois, il s'agit d'une question assez difficile. Si l'on part de la violation, je sais fort bien qu'il y a sûrement à Ottawa des endroits où un cas de violation ferait beaucoup plus de bruit qu'ailleurs, et je ne veux manquer de respect à personne en disant cela, par exemple à la Défense nationale ou à la GRC. Ici encore, il s'agit d'une question absolument fondamentale mais pour laquelle aucune réponse facile ne peut être avancée. Nous sommes simplement partis du principe que le branchement illicite à l'ordinateur est un cas de violation, mais peut-être devrions-nous aller un peu plus loin et penser à ce qui se produirait dans le cas de quelqu'un qui fait partie du système, ce serait alors, si vous voulez, le second niveau d'infraction. Vous avez parfaitement raison, monsieur Beatty, pour ce que vous dites—il faut être en mesure de faire la différence au niveau des intentions—c'est cela que vous vouliez dire, je pense—des intentions de celui qui se branche sur l'ordinateur . . .

M. Beatty: Pas nécessairement. Même dans le cas d'un petit resquilleur, j'aurais tendance à considérer l'infraction comme étant beaucoup plus grave si cet acte de resquillage débouchait sur mettons l'effacement d'une partie de la mémoire, avec pour conséquence la faillite de l'entreprise; ce serait beaucoup plus grave qu'une simple utilisation illicite du temps de l'ordinateur.

M. Ward: Je vais poursuivre en disant que si l'on part du premier niveau, c'est-à-dire le branchement si vous voulez, le second niveau serait l'utilisation que le coupable ferait de ce branchement. Prenez le cas de mon client, je vous en ai déjà parlé: en apparence, la mémoire n'a pas été endommagée. A ce

[Texte]

addressed, the definition of what causes damage. Number one, one could change the data. It is very simple to determine. One could compare the data possibly to the last time one knew what it was, from what one calls in the trade a backup of the data. Again, something which may be a little more difficult task as more systems become instantaneous or what we call real time systems. So number one is damaging the data.

• 1600

Physically changing the data is the next step. Now the question becomes: Is that data just scrambled around for malintent, or is it changed in a calculated manner, for example, to defraud? Then we start moving into the use of the computer as an instrument of a crime, and I think that is covered relatively well in legislation.

Mr. Beatty: You cautioned us, though, about attempting to quantify the worth of the data. I can certainly see the concern there; it is something we have been struggling with. It is not clear whether you assign some sort of market value to something which would not be sold; whether it is worth the cost in terms of man-years; or whether you can assign some intellectual value to data which may have some creative value in itself. But surely at some point the question arises if a data base is wiped: What sort of real damage has been done to individuals or to corporations as a result of manipulation of data? You initially talked about unauthorized access and that is the simplest thing. Then you talked in terms of intent, and I think it is fair ball to consider that and whether or not there was malicious intent there of some sort. Third, you talked about the question of whether or not there was alteration of data. But one would even see different degrees of severity where the data base was altered, depending on the injury done to the owner of the data base. You could have a data base being altered, which could cost a person his life. If it had something to do with air traffic control, for example, it could lead to an air traffic control system going down. That would certainly be more serious than my borrowing your micro and wiping a list of what you have in your freezer at home. I think inevitably you find yourself drawn into the question of evaluation of data which, as you point out, is a very difficult area. But are you saying that we should avoid—period—getting into evaluation, or if we do get into it, how do you value it?

Mr. Ward: That is the complex issue I was referring to earlier, once one starts valuing data in a computer. Many people have very great difficulty valuing data in computer when one is coming to a costs—benefit analysis of whether or not to put a computer system in. One only has to read the press generated about the Canada Mortgage and Housing Corporation recently. They talk about value of computer systems and value of making good decisions.

[Traduction]

moment-là, la question suivante qu'il faudrait approfondir serait la définition de ceux qui causeraient un préjudice. Quelqu'un pourrait par exemple, et c'est le premier cas, manipuler les données. C'est bien facile. On peut comparer les données à celles du système auxiliaire, comme on l'appelle dans le métier, qui a servi la dernière fois. Cela peut devenir un peu plus problématique dans la mesure où de plus en plus de systèmes sont instantanés ou fonctionnent en phase réelle. Alors la première chose, c'est l'endommagement des données.

Ensuite, il y a la manipulation des données. Et la question qu'on doit se poser est la suivante: pourquoi sont-elles altérées, est-ce involontaire ou délibéré par exemple? Cela nous amène à l'utilisation de l'ordinateur en tant qu'instrument du crime, et je pense qu'il existe à cet égard des dispositions relativement efficaces dans la loi.

M. Beatty: Vous nous avez parlé des difficultés inhérentes à la quantification de la valeur des données. Je n'ai pas de mal à comprendre, c'est une question que nous avons déjà abordée. Que faut-il faire? Attribuer une certaine valeur marchande à quelque chose qui n'était pas destiné à être vendu; déterminer les coûts en termes d'années-personnes, ou attribuer une certaine valeur intellectuelle à des données susceptibles d'avoir une certaine importance sur le plan de l'innovation. La question doit sûrement se poser lorsqu'on se fait voler une base de données: quel genre de dommages ont été causés à des individus ou à des sociétés par suite de la manipulation de données? Vous avez d'abord parlé d'accès non autorisé, et c'est ce qu'il y a de plus simple. Ensuite, vous avez parlé d'intention, et je pense que c'est juste qu'on en tienne compte et qu'on cherche à déterminer s'il y avait vraiment intention criminelle. En troisième lieu, vous avez parlé de la question de savoir s'il y avait effectivement altération des données. Mais il y aurait différents degrés de gravité selon les préjudices causés au propriétaire de la base de données. L'altération d'une base de données pourrait causer la mort de quelqu'un. Dans le domaine du trafic aérien, par exemple, tout le système de contrôle pourrait tomber par suite d'un changement de données. Cela serait certainement plus grave que si j'empruntais votre micro-ordinateur et que je prenais une liste de ce que vous avez dans votre congélateur à la maison. Je pense qu'on doit inévitablement en venir à la question de l'évaluation des données et, comme vous l'avez mentionné, c'est très difficile. Mais, est-ce que vous nous dites d'éviter, un point c'est tout, de faire des évaluations, ou alors si nous en faisons, comment procéder?

M. Ward: C'est le problème complexe dont je parlais tout à l'heure, une fois qu'on commence à attribuer une valeur aux données d'un ordinateur. Beaucoup de gens ont énormément de difficultés à établir la valeur des données lorsque vient le temps de faire une analyse de rentabilité avant de décider de se procurer un système informatique. On n'a qu'à lire les journaux publiés dernièrement au sujet de la Société canadienne d'hypothèques et de logement. On parle de la valeur des systèmes informatiques et de l'importance de prendre de bonnes décisions.

[Text]

So when we are talking about value of data, I think that would be difficult, if not impossible, for the subcommittee to really come to grips with because of the total range of potential values of data. I mean, from going in to change what is basically internal data, for example, to the computer systems people who are storing just some information on their documentation of the computer program on the one hand, right through, as you suggest, to air traffic. Maybe I could suggest medical records, for example, on a hospital computer, where they hold the blood type and possibly the dosage too to give to an individual. If I really wanted to take it to an extreme in one dimension, or to the financial data in another dimension, which the banks or the financial institutions keep. So if one were to attempt to value that data, I would suggest one might take from now until the year 2000 to come up with an algorithm of how one valued data.

These are some very off-the-cuff comments in valuing data, but it is really what the data is used for, which I think was the point you were getting at a few minutes ago, Mr. Beatty. What is that information used for? And maybe at that point one could attempt to start putting value on data. What is the data on the internal documentation of a computer program, which is held on a computer, used for? What is the data on a person's medical record used for? What is the result of modifying that data? Maybe there are various classification levels, if I can use that word, although that tends to conjure up secret and top secret clearances. But I mean a different type of classification of information, or classification of data, that one could consider related to what it is used for and to its value to the organization.

Mr. Beatty: Useful by its owner or by the thief?

Mr. Ward: No. Useful very much by the owner.

Mr. Beatty: What about if it is worth more to the thief than it is to the owner? You could take, for example, a mailing list I would have for my riding association. I could reconstruct it fairly easily. It might be of more use to someone else than to me.

• 1605

Mr. Ward: I would hate to suggest someone might steal the address list for your riding, Mr. Beatty.

Mr. Beatty: So would I.

Mr. Ward: Again, it is a matter, I would suggest, of trying to bring simplicity into the situation as opposed to complexity. I still suggest that maybe it is of value to you initially because we are stealing from you. This is the parameter around which we work. We attempt to quantify that. If we go into the next dimension of quantifying value to the user at that point, I think we are adding an extra degree of complexity which will make it more difficult to implement legislation.

Mr. Beatty: Two other questions. I realize I am taking up a great deal of the subcommittee's time and I appreciate the indulgence of my colleagues. The first is, you alluded to the fact that, particularly in the joy-riding type of offence, you felt a good amount went unrecorded. However, in your presenta-

[Translation]

Alors, je pense qu'il serait difficile, voire impossible, pour le Comité de vraiment trancher la question de la valeur des données, compte tenu de toutes les possibilités de valeur qu'on peut leur attribuer. Il y a les cas de ceux qui altèrent des données essentiellement internes, par exemple, les cas des informaticiens qui prennent certaines données pour la documentation de leur programme informatique, et cela peut aller jusqu'au trafic aérien, comme vous l'avez mentionné. Je pourrais peut-être parler de dossiers médicaux, par exemple, intégrés à l'ordinateur de l'hôpital où l'on retrouve le type sanguin d'un individu et peut-être les doses qu'on doit lui administrer. Je pourrais vous parler aussi des données financières des banques et des institutions financières. Alors, si on tient à établir la valeur de ces données, on sera en l'an 2,000 et on n'aura peut-être pas encore de formules d'évaluation.

Ce sont des observations qui valent ce qu'elles valent, mais je pense que l'important, c'est l'utilisation qu'on fait des données, comme vous l'avez dit il y a quelques instant, monsieur Beatty. A quoi sert l'information? Et à partir de ce moment-là, on peut peut-être commencer à attribuer une valeur aux données. A quoi servent les données d'un programme informatique intégrées à l'ordinateur? A quoi servent les données du dossier médical d'une personne? Quelle conséquence entraîne la modification de ces données? Il y a peut-être différents niveaux de classification de l'information, si je puis m'exprimer ainsi, et cela nous amène aux données classées «Secret» ou «Très secret». Je parle d'un type différent de classification de l'information ou des données, qui serait fonction de l'utilisation qu'on en fait et de leur importance pour l'organisation.

M. Beatty: Utile pour le propriétaire ou pour le voleur?

M. Ward: Non, utile pour le propriétaire.

M. Beatty: Mais qu'arrive-t-il si c'est plus utile pour le voleur que pour le propriétaire? Prenez par exemple ma liste d'envoi pour ma circonscription. Je pourrais assez facilement la refaire. Mais elle pourrait être beaucoup plus utile pour quelqu'un d'autre.

M. Ward: Je n'ose même pas penser que quelqu'un pourrait voler la liste d'envoi de votre circonscription, monsieur Beatty.

M. Beatty: Moi non plus.

M. Ward: Je le répète, je pense qu'il faut tenter de simplifier les choses plutôt que de les rendre plus compliquées. Cela a peut-être une valeur pour vous parce que vous êtes la victime du vol. C'est en fonction de cela que nous travaillons. Nous essayons d'y attribuer une valeur. Si nous y ajoutons une autre mention, celle de la valeur pour l'utilisateur, alors là nous ajoutons un degré de complexité qui rendra encore plus difficile l'application de la loi.

M. Beatty: Deux autres questions. Je sais que je prends beaucoup de temps et j'apprécie l'indulgence de mes collègues. La première: vous avez dit que, particulièrement dans les cas de resquillage, bon nombre des infractions n'étaient pas signalées. Cependant, dans votre mémoire, vous semblez dire

[Texte]

tion to us you tended to downplay what you called "inflated claims" about unreported crimes. What ratio would you assign to unreported crimes if you dispute Mr. Parker's ratio?

Mr. Ward: I hope I used the words "could go unreported" because, again, I would not say that joy riding, so to speak, would go unreported. We do not know, I guess, is the point, Mr. Beatty. I think it could go unreported. As for the percentage of crime not reported, I would not even hazard a guess, as I am not an expert on the criminal mind. I would say it is relatively low. Again, another fact is that in Toronto, both the Ontario Provincial Police and the RCMP are each investigating the grand total of one computer crime each, at this moment in time, as of a month or so ago. I would suggest there are one or two other so-called computer crimes or illegal accesses which took place. We could change that to a ratio of one to five very easily, because I do not think the population of reported cases is that large. I would not want to say this 20% is unreported, or 5% . . . I literally have no idea. I would say in 10 years of consulting to hundreds of clients, we have only come across one case which was unreported because the client felt no damage had been done, and it was a little late by that point. It went unreported to the law enforcement authorities. It was reported to the telephone companies in an attempt to apprehend the person perpetrating the crime. I must apologize, but I just cannot come out with a number as a wild guess—because that is all it would be. It would be a wild guess.

Mr. Beatty: One final question before I pass to my colleagues. One of the criticisms made about my bill and about similar approaches to dealing with the issue is that it would differentiate between data stored electronically and data stored in a manual form. You are talking about creating what would be essentially a new offence, even if you go to the question of unauthorized access, a computer trespass, if you like. Why should you treat data held in machine-readable form in a different way than data held in a filing cabinet? And, if you would not, what would be the analogous offence if I were just thumbing through your filing cabinet and I had access to your office?

Mr. Ward: You have put a very good analogy of looking at computer data and looking at filing cabinet data. One can go back and look at the mystery books one reads about spies microfilming with a small camera the data in the top-secret cabinets. I would suggest that is a very good analogy and there is little difference between the two. Typically, if one were looking at the government, for example, and one did that, one would be covered, I assume, under the various levels of classification of data. So, if one went through a secret filing cabinet one would then be prosecuted under the appropriate . . .

Mr. Beatty: Yes, the Official Secrets Act. But if it were commercial data, or, for example, if you were a reporter . . . you have a file folder in front of you now. I do not know the worth of the information in that file folder either to you or to me; but if you were to leave the room for a minute and I were

[Traduction]

que le nombre de crimes non signalés est prétendument exagéré. Quel pourcentage des crimes ne sont pas signalés, selon vous, si vous n'êtes pas d'accord avec le chiffre de M. Parker?

M. Ward: J'espère que j'ai dit «peuvent ne pas être signalés» parce que, je le répète, je ne dirais pas que les cas de resquillage ne sont pas signalés. Nous ne le savons tout simplement pas, monsieur Beatty. Je pense que ces crimes pourraient ne pas être signalés. Pour ce qui est du pourcentage de crimes non signalés, n'étant pas criminologue, je n'oserais même pas donner un chiffre. Je dirais que le pourcentage est assez faible. À Toronto, depuis un mois environ, la Sûreté provinciale de l'Ontario et la GRC mènent au total chacune une enquête sur le crime informatique. Il y a peut-être un ou deux autres cas d'infraction reliés à l'informatique ou d'accès illicite, mais c'est tout. On pourrait parler d'un rapport de un sur cinq, sans difficulté, parce que je ne crois pas que le nombre de pertes signalées soit tellement élevé. Je ne voudrais pas dire que 20 p. 100 des cas ne sont pas signalés, ou 5 p. 100 . . . car je ne sais vraiment pas. Depuis dix ans que nous offrons des services-conseils à des centaines de clients, nous n'avons eu qu'un seul cas d'infraction qui n'a pas été signalé parce que le client estimait qu'il n'y avait pas eu de dommages, et de toute façon, il était déjà un peu trop tard pour signaler le crime. Alors, l'infraction n'a pas été signalée aux autorités. Elle a été signalée aux compagnies de téléphone pour qu'on puisse appréhender l'auteur du crime. Alors, je vous prie de m'excuser, je ne peux vraiment pas vous donner de chiffres parce que ce serait purement spéculatif.

M. Beatty: Une dernière question avant de céder la parole à mes collègues. L'une des critiques au sujet de mon projet de loi et d'autres initiatives du genre sur la question est que l'on ferait une distinction entre les données emmagasinées électroniquement et les données entreposées manuellement. Vous dites que cela créerait une nouvelle infraction, même s'il n'était question que d'accès non autorisé ou de violation informatique, si vous voulez. Pourquoi faudrait-il considérer les données ordinolinguées différemment des données conservées dans un classeur? Et s'il ne faut pas faire cette distinction, quelle serait l'infraction correspondante si j'étais pris à fouiller dans votre classeur et à être dans votre bureau?

M. Ward: Votre analogie entre la consultation de données informatisées et de données conservées dans un classeur est très bonne. On se rappelle les romans d'espionnage où, au moyen d'un petit appareil, on photographiait des dossiers ultra secrets. C'est une très bonne analogie, et il y a peu de différence entre les deux cas. Au gouvernement, par exemple, si quelqu'un était pris à faire cela, je pense que le degré de sécurité entourant les données y serait pour quelque chose. Alors, s'il était question de données secrètes, la personne pourrait faire l'objet de poursuites en vertu des dispositions . . .

M. Beatty: Oui, de la Loi sur les secrets officiels. Mais si c'était des données commerciales, ou prenons le cas d'un reporter . . . vous avez un dossier ouvert devant vous. Je ne connais pas la valeur que peut avoir l'information qu'il renferme pour vous ou pour moi; mais si vous quittez la salle

[Text]

to drift back and thumb through it, it is unlikely I would have committed an offence. And yet, under either the bill I am proposing, or under what you have proposed, if I were to access it in machine-readable form, I would have committed an offence.

Mr. Ward: If I could just continue my line of thought on levels of confidentiality, my earlier comments about data and trying to classify it . . . commercial data, for example; trying to classify its impact might give us a similar manner in which to judge somebody having access to it in a computer, or in a filing cabinet, if one wanted to extend it and make it an offence.

• 1610

If someone goes through a filing cabinet which contains mailing addresses in your riding association and makes a camera copy of them, is that the same offence, for example, as going through your Apple or pet computer system that you have in your office and sitting down and actually pulling it out that way? I think one should draw that comparison and say: Is there an offence committed in the second case and/or the first case?—do that sort of analogy.

I think the offence might be the fact that somebody got into your offices and looked through your filing cabinets. If you leave your filing cabinets open and have somebody in your office and you leave them there to it, maybe you were negligent, with all due respect, in allowing that person into your office and leaving them unattended. In the same way, if I had a computer system on which I was signed-on on a computer terminal and left someone at that terminal knowing how to use it, maybe I am guilty of negligence in allowing that person to get at my data.

Maybe there is not too much of a difference in those two scenarios, although, again, one could argue very strongly about the unauthorized access, as we have been doing, to the computer being just an offence.

Mr. Beatty: Thank you very much.

The Chairman: Thank you. Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman. Mr. Ward, you have indicated that you have a specialization in computers in the banking industry, and that you have been, in effect, dealing with this kind of practice, I suppose, for some 10 years. Now, what I understand from that is that you feel, with your expertise as far as the banking industry is concerned, you are on top of computer crime; that you know how to avoid computer crime or the misuse of computers where money is concerned.

Mr. Ward: I think I could certainly, if one had the time now, go into somewhat of a long dissertation on how the major financial institutions, in all of the cases I know of, have protected their computers and associated systems against computer crime, or have attempted to do that protection.

Having said that, the potential of somebody slipping up somewhere along the line is very, very high if continued vigilance is not maintained in this area.

[Translation]

pendant un moment et si j'allais fouiller dans le dossier, il est peu probable que j'aurais commis une infraction. Cependant, aux termes de mon projet de loi ou selon ce que vous avez proposé, s'il s'était agi de données ordinolingués, j'aurais commis une infraction.

M. Ward: Si vous me permettez de poursuivre sur les degrés de sécurité qui doivent entourer les dossiers, ce que je disais au sujet des données et de leur classement . . . lorsqu'on essaye de classer des données commerciales selon leur importance, cela pourrait nous aider à déterminer s'il y a infraction lorsque quelqu'un a accès à ces données, qu'elles soient ordinolingués ou conservées dans un classeur.

Si l'on photographiait la liste d'adresses de votre circonscription prise dans un classeur, serait-ce la même chose que d'obtenir la même information au moyen de votre ordinateur Apple ou de l'ordinateur que vous avez dans votre bureau? On doit comparer les deux cas et se demander: y a-t-il infraction uniquement dans le second cas et pas dans le premier?

Je pense que l'infraction pourrait résider dans le fait que quelqu'un a pénétré dans votre bureau pour consulter des dossiers dans vos classeurs. Si vous laissez vos classeurs ouverts et qu'il y a quelqu'un dans votre bureau, c'est peut-être de la négligence que de quitter le bureau sans mettre les dossiers sous clé. De la même façon, si je laisse un programme informatique dans un terminal ouvert, je suis coupable de négligence si je quitte la pièce alors qu'il y a quelqu'un là qui sait comment se servir de l'équipement.

Il n'y a peut-être pas tellement de différence dans les deux cas, bien qu'on puisse peut-être faire valoir que l'accès non autorisé à un ordinateur constitue une infraction.

M. Beatty: Merci beaucoup.

Le président: Merci. Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président. Monsieur Ward, vous nous avez dit que vous vous spécialisiez dans les ordinateurs dans l'industrie bancaire et que cela fait environ une dizaine d'années que vous travaillez dans ce domaine. Vous semblez dire qu'avec votre expérience dans l'industrie bancaire, vous ne craignez plus le crime informatique, vous savez comment le prévenir et comment prévenir aussi l'utilisation abusive des ordinateurs dans les secteurs financiers.

M. Ward: Si nous en avons le temps, je pourrais vous entretenir longuement sur les moyens qu'ont pris les grandes institutions financières pour protéger leurs ordinateurs et systèmes connexes contre le crime informatique.

Cependant, si l'on ne continue pas à être très vigilant dans ce domaine, les chances que quelqu'un réussisse à percer le système sont très très élevées.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): So your job then as a consultant is to keep them up to date on the latest ways of avoiding misuse, or computer crime as we are calling it, in whatever form it takes place, particularly with regard to the banking industry.

Mr. Ward: One of the types of things I, or we at Peat, Marwick, may be asked to do is to help a bank evaluate its current security controls on a major data processing system—such as an on-line banking system that we are all familiar with—and to recommend to that bank that this type of control-barrier, whatever word one wants to use, be put in place and maintained to protect that computer against both intentional—that is, criminal abuse . . . and accidental misuse or abuse.

Mr. Robinson (Etobicoke—Lakeshore): From your knowledge, would you say that computer crime is at this time a real problem to the banking industry?

Mr. Ward: If I define computer crime as crime occurring against the banks at this time, I would say it is a major concern of the industry and of the police that the crime should not occur. The actual occurrence of computer crime, I would suggest, is not a problem to the banks at this time. A greater problem may be some of the types of fraudulent use of funds we have heard about in the last few months to do with, for example, telephone transfers being done illegally and people making several million dollars profit out of such a situation. But, to my knowledge, I would not say that computer crime as opposed to computer controls and security is the number one concern that most banks face to do with computer systems.

Mr. Robinson (Etobicoke—Lakeshore): What your expertise is really is the prevention of computer crime in the first place.

Mr. Ward: That is correct, Mr. Robinson . . . the prevention through appropriate controls, both technical and manual on the computer.

Mr. Robinson (Etobicoke—Lakeshore): Are you also concerned about the detection of crime, and ways to detect computer crime; that is whether the data bank has been sampled, or changed, or whatever may have been done?

• 1615

Mr. Ward: One of the preventative programs we promote with our clients has 10 components to it; and each component deals with either the manual side of the interface of the computer, the telecommunications with the computer, the data base or whatever. The types of controls we put in place are to both prevent the unauthorized access taking place in the first place, and if such access should somehow take place through a failure of control—by the way, when I say a failure of control, it could easily be a manual control failing, for example, where somebody did not take an action based on information the computer gave them—if such a control breakdown occurs, that can be detected through a normal management process within that bank; for example, the checks and balances that are done daily in a bank. There are many manual checks and balances

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Alors votre travail, en tant que conseiller, c'est de les tenir au courant des dernières techniques pour prévenir l'utilisation abusive ou le crime informatique, comme on l'appelle, particulièrement dans l'industrie bancaire.

M. Ward: L'une des choses que moi ou Peat et Marwick pouvons être appelés à faire, c'est d'aider une banque à évaluer ses systèmes de contrôle rattachés à un système informatique—comme le système de transactions bancaires directes que nous connaissons tous, et de recommander à cette banque d'installer un système de contrôle, si vous voulez, pour protéger l'ordinateur contre des utilisations abusives intentionnelles, c'est-à-dire des utilisations criminelles, et contre les utilisations abusives accidentelles.

M. Robinson (Etobicoke—Lakeshore): D'après vous, le crime informatique est-il en ce moment un véritable problème pour l'industrie bancaire?

M. Ward: Si je prends le crime informatique comme un crime contre les banques, je pense que l'industrie et la police sont aux prises avec un grave problème. La fréquence du crime informatique ne constitue pas un problème pour les banques en ce moment. Il y a un problème plus sérieux pour les banques: les différents types de fraudes dont on a entendu parler dans les derniers mois concernant, par exemple, les transferts illégaux de fonds par téléphone, qui permettent à certains de réaliser des profits de plusieurs millions de dollars. Mais, d'après moi, je ne dirais pas que le crime informatique est un grand problème, je dirais plutôt que les systèmes de contrôle et de sécurité sont la préoccupation première de la plupart des banques en ce qui concerne l'informatique.

M. Robinson (Etobicoke—Lakeshore): Votre spécialité donc, c'est avant tout la prévention du crime informatique.

M. Ward: C'est exact, monsieur Robinson . . . La prévention grâce aux contrôles appropriés, tant techniques que manuels.

M. Robinson (Etobicoke—Lakeshore): Vous intéressez-vous aussi au dépistage du crime, aux façons de déceler le crime informatique; les banques de données copiées ou altérées ou ce que vous voulez, cela vous intéresse?

M. Ward: L'un des programmes de prévention que nous proposons à nos clients comporte dix éléments, et chacun vise un aspect particulier du domaine, soit les mesures de contrôle manuel, les télécommunications, la base de données et ainsi de suite. Les types de contrôle que nous mettons en place visent d'abord à prévenir l'accès non autorisé au système et, en deuxième lieu, à signaler toute panne du système de contrôle. Par cela, j'entends une erreur sur le plan des contrôles manuels, par exemple, lorsque quelqu'un n'obéit pas à des instructions que lui donne l'ordinateur—une telle panne de contrôle peut facilement être décelée par la voie du processus de gestion ordinaire de la banque; soit par les vérifications qu'on effectue quotidiennement. Il y a de nombreuses vérifications manuelles des calculs qui permettent de s'assurer que le

[Text]

of totalling various numbers together to ensure that what happened on day one, plus or minus what happened on day two, equals what we start day three with.

Mr. Robinson (Etobicoke—Lakeshore): From your knowledge, do banks generally have a back-up system, and do they check this frequently?

Mr. Ward: It is very difficult to speak in generalities; but in general terms, the banks have very sophisticated controls in these areas; back-up systems being one, a second being a tremendous amount of manual checking to make sure the computer did the right thing or it was not illegally accessed.

For example, you may be aware of a computer crime that occurred in Calgary with one of the major banks, with the automated teller machines. That was prosecuted by the Calgary Police Department. Again, it was picked up by what I would call a detective control. The reason it occurred in the first place is because two of the many controls surrounding that computer system were not maintained by an individual. Unfortunately, the fallible human being was the problem in that case.

So the controls they had in place failed the first time around in the prevention; but in the detection that eventually did take place, I believe, two weeks after the first case took place, the person was apprehended, based on the detective type of controls.

Mr. Robinson (Etobicoke—Lakeshore): Then you do have a program of prevention and a program of detection, as far as computer crime is concerned.

Mr. Ward: Yes. I would suggest that most banks—just speaking on banks for a second—have those types of programs in place at the moment; and those programs are initiated by many different people, from the inspection departments of banks, which typically have data processing professionals in place solely for the reason of ensuring security of the computer, through to the normal auditors and the normal banking personnel, whose job it is to ensure on a day-to-day basis that the business is run according to standards and according to normally accepted accounting principles.

Mr. Robinson (Etobicoke—Lakeshore): Your specialization is with computer banking or the banking industry. What are some other areas of specialization as far as computers are concerned? If you are dealing just with the banks, then there is a whole lot of others out there. What other areas of specialization are there? What other specialists should we be having before this committee, for instance, to give us additional information, apart from what you are able to give us through the banking industry?

Mr. Ward: Two groupings come to mind immediately. One—I assume this is covered off—is the law enforcement agencies, the RCMP. You have a submission from Superintendent Allen. One should attempt, I would suggest, to talk to the people who are—if I can use the word—at the sharp end of criminal investigation in the computer area; and there are several people I know of in the RCMP and the Ontario

[Translation]

total de la première journée plus ou moins le total de la deuxième journée égale le montant qu'on aura au début de la troisième journée.

M. Robinson (Etobicoke—Lakeshore): D'après vous, les banques ont-elles généralement un système d'appoint, et le vérifie-t-on fréquemment?

M. Ward: Il est très difficile de parler de généralités; mais les banques disposent de contrôles très sophistiqués dans ces domaines; les systèmes d'appoint en sont un élément, les nombreuses vérifications manuelles permettant de déterminer si l'ordinateur fait la bonne chose ou s'il n'a pas été utilisé illégalement en sont un autre.

Par exemple, vous êtes peut-être au courant du crime informatique concernant l'une des grandes banques à Calgary impliquant les guichets automatiques. L'auteur du crime a été appréhendé par le service de police de Calgary. L'infraction a été décelée grâce à un contrôle de détection. Tout est arrivé d'abord parce que deux des nombreux contrôles entourant le système informatique n'étaient pas effectués par l'employé qui en était chargé. Malheureusement, le problème est imputable à une erreur humaine.

Les mesures de contrôle en place n'ont pas réussi à prévenir le crime, mais les systèmes de dépistage ont permis d'appréhender l'auteur du crime deux semaines après la première infraction.

M. Robinson (Etobicoke—Lakeshore): Vous avez alors un programme de prévention et un programme de dépistage du crime informatique.

M. Ward: Oui. La plupart des banques, si je peux parler exclusivement des banques pour le moment, disposent actuellement de ces programmes; et ces programmes peuvent être mis sur pied par de nombreuses personnes, depuis les spécialistes de l'informatique des services d'inspection des banques qui sont chargés exclusivement de la sécurité des systèmes informatiques, jusqu'aux vérificateurs et aux employés ordinaires de la banque qui doivent s'assurer au jour le jour que les affaires fonctionnent selon les normes et selon les principes de comptabilité généralement acceptés.

M. Robinson (Etobicoke—Lakeshore): Vous vous spécialisez dans les systèmes bancaires informatisés ou l'industrie bancaire. Quels sont les autres domaines de spécialisation en ce qui concerne les ordinateurs? Si vous ne vous intéressez qu'aux banques, il reste beaucoup d'autres domaines. Quels sont les autres domaines de spécialisation? Quels autres spécialistes devrions-nous inviter à comparaître pour obtenir d'autres informations en plus de celles que vous nous avez données sur l'industrie bancaire?

M. Ward: Il y a deux groupes qui me viennent immédiatement à l'idée. Le premier, je pense que vous l'avez déjà rencontré, c'est les services de l'ordre, la GRC. Vous avez reçu un mémoire du surintendant Allen. Il faudrait essayer de rencontrer les gens qui participent directement aux enquêtes criminelles dans le domaine de l'informatique; et il y a plusieurs personnes à la GRC et à la Sûreté provinciale de

[Texte]

Provincial Police, part of whose job is to get involved if a computer crime is believed to have been perpetrated.

So I would suggest, with due respect to the committee, that they should talk to people who have actually witnessed, from an independent law enforcement perspective, a computer crime and a computer crime investigation. Certainly, people with the Ontario Provincial Police, the Anti-Rackets Branch, and I am sure with various branches—I think it is A Division in Toronto, although I am not sure of the division—of the RCMP also have people who are considered initially computer-crime experts, but whose police experience obviously goes beyond that of computers. That would be one group of people I suggest one should speak to, Mr. Robinson, just to get the feeling of what really is a computer crime. What does it look like? What does it smell like? What does it feel like? Again, back to my earlier comments. I am a very practical person; I believe we should be very practical in this area and not get lost in too, too much theory.

• 1620

Mr. Robinson (Etobicoke—Lakeshore): Although there may be others, in your paper there are two quotes in particular I want to ask you about. One is on page 2, a quote within a quote, and from Donn B. Parker of SRI International, his statement dated December 10, 1979. It says, "In my book, 'Crime by Computer'..." and *Crime by Computer* in quotes—is it fair to say that crime by computer is the same thing as computer crime?

Mr. Ward: I think so. The book in question was published in 1976. Again, Donn Parker makes a lot of money by selling books on computers, and particularly computers involved in crime. Though I have not more than scanned that book, I assume that crime by computer is his way of making the words "computer crime" a little bit more exciting.

Mr. Robinson (Etobicoke—Lakeshore): It seemed to me that it was maybe more limited than computer crime. Crime by computer means, in my view, that you can get a computer to perform the computer crime, which may limit. Do you feel there are limitations? Do we not have a broader concept when we talk about computer crime?

Mr. Ward: Oh, I think the concept you are talking on in this committee, as defined to me by Mr. Beatty and defined in Superintendent Allen's paper, is the broadest possible concept we could consider. I know that in Mr. Parker's writings he also uses the words "computer abuse"; i.e., the abuse of a computer, which I understand is the same definition you are using, where the computer is both the object of the crime and the instrument of the crime.

Mr. Robinson (Etobicoke—Lakeshore): Yes. And on page 3, at the bottom, the second last line, you say:

[Traduction]

l'Ontario qui sont chargées d'effectuer les enquêtes dans le domaine du crime informatique.

Je suggérerais au Comité de rencontrer des personnes, indépendantes des services de l'ordre, qui ont vraiment été témoins d'un crime informatique et qui ont participé directement à l'enquête. Il y a sûrement des agents de la Sûreté provinciale de l'Ontario, du Service de lutte contre les rackets, et de nombreux autres services—je pense qu'il y a la Division A à Toronto, je n'en suis pas certain, la Division A de la GRC qui a des spécialistes du crime informatique, sans que leur expérience se limite à ce domaine. C'est un groupe de personnes que je vous suggérerais de rencontrer, monsieur Robinson, pour que vous sachiez vraiment ce que c'est un crime informatique. Pour que vous en connaissiez tous les détails. Une fois encore, pour en revenir à ce que je disais plus tôt, je vois les choses sous l'angle très pratique et je pense que dans ce domaine, nous devons garder notre sens pratique et ne pas nous laisser dépasser par trop de théorie.

M. Robinson (Etobicoke—Lakeshore): Vous avez cité dans votre exposé, entre autres, deux extraits à propos desquels j'aimerais vous poser des questions. Il y a d'abord à la page 2 une citation dans une autre citation que vous attribuez à Donn B. Parker de la Maison SRI International, une citation en date du 10 décembre 1979 qui dit ceci: dans mon livre intitulé «*Crime by Computer*»... le titre est entre guillemets, peut-on vraiment affirmer que le crime par ordinateur soit la même chose que le crime informatique?

M. Ward: C'est ce que je dirais en effet. L'ouvrage en question a été publié en 1976. Donn Parker gagne beaucoup d'argent en écrivant et en publiant des livres sur les ordinateurs et en particulier sur les ordinateurs utilisés à des fins criminelles. Même si je n'ai fait que parcourir rapidement ce livre, je suppose que lorsqu'il parle du crime par ordinateur, c'est une façon pour lui d'attirer davantage l'attention sur le crime informatique.

M. Robinson (Etobicoke—Lakeshore): Il m'avait semblé que cette acception était un peu plus limitée peut-être que le crime informatique proprement dit. Le crime par ordinateur signifie, à mon avis, l'utilisation par quelqu'un d'un ordinateur pour perpétrer un crime informatique, ce qui pourrait être limitatif. Est-ce que vous avez le même sentiment que moi? Le fait de parler de crime informatique ne nous donne-t-il pas une notion plus générale?

M. Ward: Ecoutez, je vous dirai que la notion dont vous parlez ici au Comité et qui a été définie à mon intention par M. Beatty et également par un exposé de M. Allen, est en fait la notion la plus générale possible. Je sais que M. Parker parle également dans ses ouvrages d'«utilisation abusive des ordinateurs», ce qui selon moi ressemble à la définition que vous utilisez dans la mesure où l'ordinateur est à la fois la victime et l'instrument de l'acte criminel.

M. Robinson (Etobicoke—Lakeshore): D'accord. A la page 3, vers la fin de la page, vous dites à l'avant-dernière ligne:

[Text]

On the other hand, a potential does exist, as more and more of our lives become "computerized", for major computer fraud to occur.

And the word "computerized" is in quotes. Now, what is your meaning of that? If you put it in quotes, I assume it has a special meaning to you, or you have taken it from some context, or out of context, or from some writing or something; what meaning does this have?

Mr. Ward: Perhaps I was being a little objective here. I hate to use the word "computer" in the context of computerizing an individual. Although 1984 is less than a year away, I hate the thought of an individual being computerized.

What I was attempting to get at is that more and more each day we come into contact with a computer. Today I have come into contact with at least three computers since I left home in Toronto this morning. I flew to Montreal first thing this morning and Air Canada's computer gave me a boarding pass. I came on VIA rail at lunchtime, and that gave me a ticket. Then I went to the Bank of Commerce, used my VISA card and drew out \$100. So we are coming closer and closer.

I think the point I am getting at, Mr. Robinson, is that computers are playing an increasing part in our lives. More and more we access them ourselves, the general public has access to the computer. When one thinks of the automated teller machines in the bank, it is the only case I know where you or I could walk up and take, or in fact steal, \$200 without anybody knowing it. Anybody in this room could go to a bank and open an account, and in a lot of cases one does not need to have that \$200 actually in one's account when one takes it out of the automated teller machine—as our friend in Calgary who took \$1,500 did not have \$1,500 in the account. So for the first time in our lives we do not have to go into a bank or into the corner store with a drawn gun and threaten and take the money out of the till. We simply walk up to an inanimate object, with nobody else around, feed in a little card, key in a couple of numbers and out comes \$200. That is somewhat frightening, when it is not necessary to have that \$200 in the bank in the first place. That is just one example of how we are becoming, to use my word in quotes, "computerized" as individuals.

If one takes that further, in talking to enforcement officers, police officers, the biggest concern the police forces have in this area is that given all the money that a bank computer controls, somebody at some point will work out a way not to get \$1,500 but to get millions of dollars out of a bank's computer. I am sure you are all familiar with the situation at one of the Toronto banks where a telephone transfer from Montreal resulted in an individual getting away with several million dollars fraudulently. Again, not computer crime, but potentially it could just as easily have been a computer crime if a computer terminal had been involved, as opposed to a

[Translation]

D'autre part, les possibilités restent entières dans la mesure où la vie devient de plus en plus «informatisée», possibilités d'une fraude d'envergure perpétrée par ordinateur.

Et vous mettez entre guillemets le mot «informatisée». Qu'entendez-vous par là? Si vous l'avez mis entre guillemets, je suppose que vous prêtez à ce terme une signification particulière, à moins que vous l'ayez repris d'une autre source ou cité hors contexte, que sais-je? Qu'entendez-vous par là?

M. Ward: Peut-être ai-je été un peu objectif. J'ai horreur du mot «ordinateur» appliqué à la mise sur ordinateur de la personne. Même si 1984 est quasiment à la porte, la seule pensée de mettre les gens sur ordinateur me fait horreur.

Ce que j'ai essayé de dire, c'est que chaque jour qui passe nous rapproche davantage de l'ordinateur. Aujourd'hui, depuis que j'ai quitté ma maison ce matin à Toronto, j'ai été trois fois en contact au moins avec l'ordinateur. En début de matinée, j'ai pris l'avion pour Montréal et l'ordinateur d'Air Canada m'a délivré ma carte d'embarquement. À midi, j'ai pris le train pour Ottawa et VIA Rail m'a délivré un billet par ordinateur. Je me suis ensuite rendu à la Banque de Commerce, j'ai sorti ma carte VISA et j'ai fait un retrait de 100 dollars. L'ordinateur est donc de plus en plus proche de nous.

Ce que je veux dire, monsieur Robinson, c'est que l'ordinateur joue un rôle de plus en plus important dans notre vie quotidienne. De plus en plus nous l'utilisons nous-mêmes et de plus en plus le grand public en général peut se servir de l'ordinateur. Pensez simplement aux guichets informatisés des banques; je pense que c'est le seul cas auquel je puisse penser où n'importe qui peut effectivement arriver à voler 200 dollars et repartir sans que personne ne remarque quoi que ce soit. N'importe qui ici peut aller à la banque, s'ouvrir un compte, et dans la plupart des cas, il ne faut même pas 200 dollars dans son compte pour pouvoir retirer 200 dollars du guichet automatique: souvenez-vous de notre ami à Calgary qui a retiré ainsi \$1,500 qu'il n'avait pas à son compte. Pour la première fois donc, dans notre existence, nous ne devons plus aller braquer une banque ou une épicerie et brandir un revolver pour vider le tiroir-caisse. Il suffit de se placer devant cet objet inanimé, à une heure creuse, d'introduire une petite carte en plastique, d'appuyer sur quelques touches et voilà, on a 200 dollars. C'est un peu effrayant, ne trouvez-vous pas, surtout lorsqu'on pense qu'il ne faut même pas avoir 200 dollars dans son compte pour le faire. Voilà un exemple de cette informatisation, pour reprendre mon expression, de la personne humaine.

Si l'on va un peu plus loin, si l'on en parle aux représentants de l'ordre, aux corps policiers, on se rend compte que ce qui les inquiète le plus, c'est que, avec tout cet argent qui est contrôlé par les ordinateurs des banques, il se peut fort bien qu'à un moment donné quelqu'un parvienne à prélever non pas \$1,500, mais des millions et des millions. Vous êtes tous, j'imagine, au courant du cas d'une de ces banques de Toronto qui a perdu plusieurs millions de dollars qui leur ont été soutirés frauduleusement par un simple virement téléphonique depuis Montréal. Ici aussi, ce n'est pas à proprement parler un crime informatique, mais ça aurait facilement pu l'être si le criminel

[Texte]

telephonic transfer of money with, I believe, a certain code system which somebody had.

• 1625

Mr. Robinson (Etobicoke—Lakeshore): But are they not set up with safeguards so that over a certain amount a red light goes on someplace or a bell rings or there has to be a double check or there is a new code fed into it or something?

Mr. Beatty: The computer is often down, though, in the p.m..

Mr. Ward: I prefer not to go into the details of automated teller machines. I think I might suggest some ways that have been used in the past. In fact, there was one publication, to digress slightly, produced in the United States for \$18, I believe, *100 Ways to Beat your ATM*, and there were 100 ways listed in this publication, once automated teller machines were initially installed, on how to beat them. One of the ways, of course, was to drive a truck up and pull the thing out of the wall, but there were many ways on how to use that automated teller machine to get money and to continue to get money without being detected if one knew certain ways it worked.

Mr. Robinson (Etobicoke—Lakeshore): Just one further area I wanted to ask you about. Mr. Beatty talked about computer trespass and was relating that to illegal access to the computer. It would seem to me that if we try to analogize we have, say, the Petty Trespass Act of Ontario, and if you violate that you would be fined or something but you would not have a criminal record. On the other hand, if you are charged under the Criminal Code for trespass, you would end up with a criminal record.

So it makes a great deal of difference, and on occasion I have had cases of that nature where people were charged either under the Petty Trespass Act or they were charged under the Criminal Code; it makes a big difference.

Are you suggesting or would you suggest that we should amend the Criminal Code to have a section pertaining to computer crime so there would be a conviction attached to it and along with the conviction a record? Or would you suggest just a federal statute, or maybe provincial statutes as well, or maybe a meeting of the provinces and the federal government to decide who should have total jurisdiction in the area if it is outside of the Criminal Code?

What do you actually see as the approach to take?

Mr. Ward: I must apologize, Mr. Robinson, for not being a lawyer or really understanding in detail the way in which we structure the various aspects of our criminal legislation. You started off with petty trespass and maybe several categories of trespass... I think that is what you were referring to—one of which results in a criminal record. It is almost like driving a car. You can do everything from break the speed limit by 10 kilometres an hour...

[Traduction]

avait utilisé un terminal d'ordinateur plutôt qu'un téléphone et un certain code pour effectuer son virement.

M. Robinson (Etobicoke—Lakeshore): D'accord, mais n'y a-t-il pas des dispositifs de sécurité, par exemple je ne sais pas une lampe rouge qui s'allume quelque part ou une sonnette qui se mette à résonner ou encore une double vérification, un nouveau code, que sais-je?

M. Beatty: Il arrive souvent que l'ordinateur ne fonctionne pas le soir...

M. Ward: Je préférerais ne pas m'étendre trop sur la question des guichets automatiques. Je pourrais vous parler de certains trucs qui ont été utilisés dans le passé. Pour faire une petite digression d'ailleurs, je vous renvoie à une publication américaine en vente pour 18 dollars et qui s'intitulait, je crois, *100 Ways to Beat your ATM* qui expliquait cent façons de rouler les guichets automatiques au moment où ceux-ci ont commencé à faire leur apparition. Bien sûr, l'une des façons consistait à utiliser un camion pour déceler la machine du mur, mais il y avait aussi toute une série de façons de retirer de l'argent à plusieurs reprises sans jamais être repéré. Il s'agissait simplement de savoir comment s'y prendre.

M. Robinson (Etobicoke—Lakeshore): Une dernière question que j'aimerais vous poser dans un autre domaine si vous voulez bien. M. Beatty a parlé de violation d'ordinateur en pensant au branchement illicite. Il me semblerait que, si nous faisons l'analogie avec mettons la loi ontarienne sur la simple violation, une infraction de ce genre ferait l'objet d'une amende sans pour autant ouvrir un casier judiciaire. En revanche, toute condamnation pour violation en vertu du Code criminel débouche directement sur un casier judiciaire.

Il y a donc une énorme différence et j'ai eu à entendre personnellement certaines causes de ce genre, deux cas de ce genre où les personnes étaient poursuivies pour violation en vertu de la loi ontarienne ou du Code criminel, et la différence est flagrante.

Devrions-nous, selon vous, modifier le Code criminel en y ajoutant des dispositions relatives au crime informatique, ce qui s'assortirait à la fois de peine et de casier judiciaire, ou au contraire vous satisferiez-vous d'une simple loi fédérale, voire provinciale, qui pourrait être le résultat d'un accord entre le gouvernement fédéral et les provinces quant au niveau de juridiction à cet égard puisqu'il ne s'agirait pas d'un domaine couvert par le Code criminel?

A votre avis, quelle serait la formule à adopter?

M. Ward: Excusez-moi, monsieur Robinson, mais je ne suis pas juriste et je ne comprends pas vraiment dans tous ses détails la structuration des divers éléments de notre législation pénale. Vous avez commencé par parler de la violation simple pour passer aux diverses catégories de violation... je pense que dans le cas dont vous parliez, il s'agissait d'une infraction donnant lieu à un casier judiciaire. C'est un peu comme quand vous conduisez votre voiture. Vous pouvez commettre un excès de vitesse en roulant dix kilomètres à l'heure plus vite que...

[Text]

Mr. Robinson (Etobicoke—Lakeshore): What I am really saying is that if there was a charge to be laid for trespass the choice in the mind of the police officer or whoever is laying the charge would be: Will I charge the fellow under the Petty Trespass Act or will I charge him under the Criminal Code?

Mr. Ward: I think that sort of . . .

Mr. Robinson (Etobicoke—Lakeshore): I am wondering, from you, if you can tell us with which kind of legislation would be most helpful in the computer field—to have an amendment to the Criminal Code or additional clauses, or to have a separate act altogether?

Mr. Ward: Again, I must admit that I am not an expert on legislation. I think we need something, such as in the Criminal Code, which would deter that person. It is not sufficient, I think, to suggest that the person who gets into joy-ride is just going to be accused of petty trespass. I think we have to have a more severe penalty. As I understand it, the Criminal Code and having a criminal offence recorded against you is more of a deterrent. That would be my only suggestion.

Mr. Robinson (Etobicoke—Lakeshore): This is my final question because I have to go to the House to speak. I want to ask you this. You talked about the definition of damage and the definition of valuation and this kind of thing. There are a number of terms that will have to be defined, and can you help us, from the point of view of being in an accountancy auditing firm like Peat, Warwick and Partners, by giving us some definitions—if not today, maybe sending us a written statement or a letter indicating what you figure should be some of the terms that should be defined insofar as computers are concerned and computer crime, which we are studying, and what the definitions should contain? I think this might be very helpful to us.

Mr. Ward: Certainly, again, it would take some time now to go into the details of that, Mr. Robinson; but I would be very pleased to take that thought away and to get back to the committee through the secretary in the next few weeks with some ideas on the results or the damage that could occur with computer crime.

I wonder if I could just add one thing. You asked who else one should speak to. I would add one other list of people, and it is very difficult, I am sure, for this group maybe to talk to them.

• 1630

There are people in the federal government who specialize in security in computers. The RCMP has an excellent group of people called the SEIT Team. Some of the best technical experts in my opinion in the country exist in that team. I would suggest if one has not already thought of those, that would be another area to pursue.

The Chairman: Excuse me. Just to complete, maybe because you are a consulting firm, I would be interested if your firm

[Translation]

M. Robinson (Etobicoke—Lakeshore): Ce que je voulais dire, c'est que si des poursuites en violation doivent être intentées, le représentant de l'ordre qui porte l'accusation pourrait avoir à se demander s'il doit invoquer la Loi sur la violation simple ou le Code criminel.

M. Ward: C'est le genre de chose qui . . .

M. Robinson (Etobicoke—Lakeshore): Vous pourriez peut-être nous dire quelle serait la mesure législative qui nous serait la plus utile dans le domaine informatique: un amendement au Code criminel ou encore des nouvelles dispositions à ajouter au Code criminel ou une loi entièrement nouvelle?

M. Ward: Je dois vous avouer ici encore que la loi n'est pas mon domaine. Ce qu'il nous faut, dirais-je, comme dans le cas du Code criminel, c'est une disposition qui aurait un effet de dissuasion. Il ne suffirait pas, je pense, de dire que le petit resquilleur va simplement être poursuivi pour violation simple. Nous devrions avoir des peines plus sévères. De la façon dont je vois les choses, une infraction punie par le Code criminel et qui ouvre sur un casier judiciaire a un effet de dissuasion beaucoup plus marqué. C'est la seule chose que j'avais à vous dire.

M. Robinson (Etobicoke—Lakeshore): Une dernière question parce que je dois prendre la parole à la Chambre: vous avez parlé de la définition du préjudice et de la définition de la valeur. Il y a plusieurs éléments qui vont devoir être définis, et puisque vous travaillez pour un cabinet comme Peat, Marwick, vous pourriez peut-être nous aider en nous fournissant quelques définitions—pas aujourd'hui, mais vous pourriez nous écrire pour nous dire quels sont les termes qui, selon vous, devraient être définis dans le domaine des ordinateurs et du crime informatique, domaines que nous étudions, pour nous dire donc quelles devraient être les définitions. Cela nous serait assurément très précieux.

M. Ward: Je le ferai avec plaisir, mais il me faudra un certain temps pour approfondir un peu les choses, monsieur Robinson, mais je me ferai un plaisir d'y penser et de reprendre contact avec vous par l'entremise du greffier d'ici quelques semaines pour vous soumettre mes idées sur les incidences ou les préjudices qui pourraient être attribuables au crime informatique.

Peut-être pourrais-je ajouter une dernière chose. Vous m'avez également demandé à qui vous pourriez vous adresser. Je vais vous communiquer une liste de gens avec lesquels vous pourriez utilement prendre contact même si vous aurez sans doute du mal à le faire.

Le gouvernement fédéral a des spécialistes en matière de sécurité des ordinateurs. La GRC a une équipe excellente qui s'appelle SEIT. À mon avis, certains des meilleurs experts techniques du pays font partie de cette équipe. Si vous n'avez pas déjà pensé à les inviter, ce serait une autre possibilité.

Le président: Excusez-moi. Puisque *Peat and Marwick* est une société d'experts-conseils, j'aimerais savoir si elle a déjà

[Texte]

was in any way a victim, not of stealing data or information from a bank but of going away with various programs that your firm has developed over the years and using them for consulting services, of course, having a chief analyst of software just making a copy of a very sophisticated program you would have developed and using it as a competitor. Do you feel you are well protected? You earn your living—your company is making a living by selling very often services analysing and of course providing people with good programs. Do you feel there is some copyright protection for the kind of services you have in your firm?

Mr. Ward: A very good question, Madam Chairman. We have not had an example that we know of of somebody taking away computer programs. We are in fact developing more and more computer programs, where in the older days, we may have developed a manual, for example, as we have with our security evaluation program. The program we have cost us close on half a million dollars to develop. When I use the word “program”, I am not referring to a computer program; it was a manual program. There is a very good chance that people, clients who have borrowed the book, have infringed the copyright. It is a confidential, not to be copied book. Or possibly people who have left the firm have taken copies with them.

The same could easily apply with the computer programs, if I can use the word “computer programs” now—that we are developing now to supplement and to take over from the more manual programs we had in the past. It is very difficult for us—it is a problem we are coming to grips with now—to copyright that type of computer program. So a lot of the time we are now using micro-computers and micro-computer software; and the stealing of micro-computer software is again, I know, of some concern to the police. There is at least one case in Canada now where nobody knows who is going to prosecute under what legislation the copying of a simple diskette of that program.

So to answer your question directly, we have no known cases where people have done that, but we are more and more concerned that the computer programs we are developing to replace our manual programs could potentially be taken. But it is very difficult to safeguard that when it is simply a program for auditing or for computer security which is on a micro-computer.

The Chairman: Yes, the government is actually revising its legislation on copyright. Certainly I was wondering if you had given your opinion to that working group within the government that is supposed to prepare a very thorough review of the copyright legislation. I had the feeling that it is certainly in that direction that... it is like the tape for tape recorders, which of course changed entirely the picture in the communications area. I presume for a firm like yours it involves several hundred thousand dollars sometimes for some of your customers to develop a comprehensive program of their information, and when they address your firm, it is to provide them with the services, and of course these can be very easily—after it has been developed by your firm and your client is using it,

[Traduction]

été victime, non pas d'un vol de données, mais plutôt d'un vol de logiciels qu'elle a élaborés au fil des ans. Il suffirait qu'un analyste de logiciels fasse une copie d'un programme très compliqué pour ensuite s'en servir en tant que concurrent. Estimez-vous que la société est bien protégée contre ce genre d'abus? Votre société fait des bénéfices en vendant des services d'analyses et en fournissant de bons programmes. Existe-t-il, à votre avis, une protection du droit d'auteur pour le genre de services offerts par votre firme?

M. Ward: Excellente question, madame le président. Que nous sachions, personne n'a encore volé de programmes d'ordinateurs. Nous élaborons de plus en plus de programmes d'ordinateurs, tandis que par le passé, nous avions plutôt des programmes manuels, comme celui de l'évaluation de la sécurité. Ce programme nous a coûté presque un demi-million de dollars. Et dans ce cas, il s'agit d'un programme manuel, et non pas d'un programme d'ordinateur. Il est très probable que les clients qui ont emprunté le livre ont violé le droit d'auteur. Le livre est pourtant confidentiel, et ne devrait pas être copié. Il est également possible que des employés qui nous ont quittés en ont apporté des exemplaires.

La même chose pourrait très bien arriver dans le cas de programmes d'ordinateurs qu'on élabore maintenant pour compléter et remplacer les programmes manuels du passé. Il nous est très difficile de protéger par un droit d'auteur ce genre de programmes d'ordinateurs, mais nous commençons à faire face à ce problème en ce moment. Très souvent, nous nous servons de micro-ordinateurs et de logiciels de micro-ordinateurs. Je sais que la police se préoccupe du vol des logiciels de micro-ordinateurs. Il existe au moins un cas au Canada à l'heure actuelle où quelqu'un a copié une disquette d'un programme, et personne ne sait qui va tenter la poursuite et en vertu de quelle loi ce sera fait.

Donc, pour répondre à votre question, il n'existe pas de tels cas chez nous à notre connaissance, mais nous sommes de plus en plus inquiets du fait que les programmes d'ordinateurs que nous élaborons pour remplacer nos programmes manuels pourraient éventuellement être volés. Mais il est très difficile de protéger un programme de vérification ou de sécurité d'ordinateurs qui se trouve dans un micro-ordinateur.

Le président: Le gouvernement est en train de réviser sa Loi sur le droit d'auteur en ce moment. J'aimerais savoir si vous avez fait des commentaires au groupe de travail qui est censé préparer une révision détaillée de la Loi sur le droit d'auteur. La situation est semblable à celle de la bande magnétique, qui a bien sûr tout à fait changé le domaine des communications. Je suppose qu'une société comme la vôtre doit parfois dépenser plusieurs centaines de milliers de dollars pour préparer des programmes pour certains de ses clients. Mais il est très facile pour quelqu'un, un ancien employé ou quelqu'un d'autre, de se servir du même programme gratuitement.

[Text]

somebody from your firm or somebody else using it might just transfer or use exactly the same program without any cost.

Mr. Ward: I am sure that will happen in the future. I am sure we will see examples of that happening. We are seeing examples of micro-computer software being copied and one change being made and the changed version being distributed. That is the case, I believe, that exists in southern Ontario now; and the question is has somebody stolen something, in that perspective? I believe several police jurisdictions have great difficulty in coming to grips with who is responsible for prosecuting, as I said, under what—whether it is a provincial or a federal statute.

The Chairman: Okay. Well, I have no further questions. Mr. Beatty, do you have a final one?

• 1435

Mr. Beatty: I have one or two points. The chairman picked up on the question of protection for software and how you would try to deal with that. One of the other areas I meant to ask you about was that one of the jurisdictions in the U.S. —I believe it may be Georgia— has a reporting requirement in the law. Have you tracked what has happened with that at all? Has it led to a significant increase in reporting; and if so, what sort of figures have come out of that?

Mr. Ward: I assume, Mr. Beatty, we are talking about a reporting requirement for an offence or computer crime.

Mr. Beatty: For people who have been victimized.

Mr. Ward: No, I am not. I was aware it had happened. We have not tracked it. I am sure that . . . Maybe the local police jurisdiction may have been; but again, it is a matter of a controlled experiment to say what would have happened if we did not have the law. What was not reported one will never know. I have no information on that beyond what my thoughts are on unreported computer crime.

I think if one adds an additional level of saying you have to report it because it is the law to report it, I would suggest that managers who are not reporting it have been even more negligent than they supposedly are today when they do not report it.

Mr. Beatty: Do you favour such a provision in the law? I understand, in the state that has it in the U.S., there is no sanction that can be taken. It is really a moral injunction that the people are to report. Do you feel one element of the computer crime law should be mandatory reporting?

Mr. Ward: Certainly, at least a moral injunction to report is needed; or not "needed", but is the strength of the case. I think building that into the law would be a good idea at this point, if one could build it in before the law is put in and one does not have to change it later.

Mr. Beatty: One of the problems with the packet switching networks is their international nature, that it is just as easy to

[Translation]

M. Ward: Je suis convaincu que cela arrivera à l'avenir. Il y aura certainement des cas de ce genre. Déjà, on fait des copies du logiciel d'un micro-ordinateur, on fait un petit changement et la version modifiée est distribuée. Mais il y a un cas de ce genre dans le sud de l'Ontario en ce moment. La question est de savoir si oui ou non il y a eu vol dans un tel cas. Je pense que la police a du mal à décider s'il s'agit d'une violation d'une loi provinciale ou fédérale.

Le président: D'accord. Je n'ai pas d'autres questions. Avez-vous une dernière question, monsieur Beatty?

M. Beatty: J'ai une ou deux questions à vous poser. Le président a déjà soulevé la question de la protection du logiciel. Dans un des États américains, je crois que c'est peut-être la Georgie, la Loi prévoit que les victimes doivent signaler les infractions à la police. Savez-vous quels sont les résultats de ce système? A-t-il entraîné une augmentation importante du nombre de cas qui sont signalés à la police? Le cas échéant, quels sont les chiffres en question?

M. Ward: Je suppose, monsieur Beatty, qu'il s'agit d'une obligation de faire rapport à la police d'une infraction en matière d'ordinateurs.

M. Beatty: Pour ceux qui ont été victimes de ce genre d'infraction.

M. Ward: Je ne suis pas au courant des résultats de cette obligation. Je sais qu'elle existe, mais nous n'avons pas fait de suivi. Peut-être que la police locale serait au courant des résultats. Il s'agit d'une expérience contrôlée pour savoir ce qui se passerait si la loi n'existait pas. On ne saura jamais combien de cas ne sont pas signalés à la police. À l'exception de mes observations au sujet des infractions d'ordinateurs qui ne sont pas signalées à la police, je n'ai pas de renseignements dans ce domaine.

Je pense qu'une loi impose quand même une obligation supplémentaire. À mon avis, les gestionnaires qui habitent un état où une telle disposition existe dans la loi, et qui ne signalent pas les infractions à la police, négligent leurs devoirs encore plus que les gestionnaires qui habitent ailleurs.

M. Beatty: Êtes-vous en faveur de ce genre de disposition? Je pense que l'état qui l'a ne prévoit pas de pénalité. Il s'agit plutôt d'une incitation morale. Estimez-vous que la Loi sur les infractions en matière d'ordinateurs, devrait obliger les victimes à faire rapport des infractions?

M. Ward: Je pense qu'il serait bon d'avoir au moins une invitation morale dans ce sens. Il serait souhaitable d'incorporer une telle disposition à la loi avant qu'elle ne soit adoptée.

M. Beatty: L'un des problèmes des réseaux de commutation de paquets est qu'ils sont internationaux. Il est tout aussi facile

[Texte]

vandalize a computer data base located in Ottawa from New York or from Bonn, West Germany, or from Sydney, Australia, as it is to do it from within Ottawa. Yet the reach of any legislation we would pass in Canada would not extend beyond our borders. What sort of international action should the Government of Canada be taking to deal with the international context of computer crime?

The Dalton School incident is a case in point, where it is debatable whether, even if an offence in Canada had been committed—and it does not appear as if one was committed in Canada—it would be debatable as to whether or not the offence was even extradictable.

Mr. Ward: That is an interesting question. Again, I do not think there is any easy answer, Mr. Beatty. The incident I mentioned at the start was a very vivid example of that, where it was traced back to the San Francisco Bay area by the telecommunications authority responsible. Even if one had identified that person, I assume that person could have only been charged with unlawful use of the telecommunications facility in the United States; i.e., the packet switching network and the access thereto.

On a multilateral basis—for example, the United States and Canada getting together—I am not sure what other parallels exist for that type of co-operation. I am trying to think quickly of what types of crime could be perpetrated in one country which affected another country; for example, the crime or occurrence physically taking place in the U.S. and the impact of the crime being in Canada. It is like someone reaching over the border to steal the money. I cannot think of any other parallels at the moment, although you may have done. But I think, again, one has to come up with some multilateral arrangements with the U.S. to come to grips with that.

Again, I suggested from my earlier comments that I think, if one gets into that area when considering legislation, one could be here for 10 years attempting to resolve it. My urging to the subcommittee, with due respect, would be to keep things relatively simple in the context to enable something to get onto the statutes relatively quickly as opposed to taking the three or four issues which really could cause problems and pursuing them, maybe to take the five basic issues and attempt to have legislation which covers those. I would suggest, by putting that legislation in, it would do more than just putting the barrier up; it would increase everybody's awareness tremendously of this area, and again, other controls would then be put in place.

Mr. Beatty: I think we have a moral effect as well in terms of society's saying to a potential joy-rider that we feel this is something that is wrong.

Mr. Ward: Yes, that is correct. As opposed to taking those next four, which it may take five years of study and legislation drafting to come to grips with, I would suggest the first five or so issues should be addressed relatively quickly, resolved, and hopefully, the safeguards put into place. I firmly believe this area is not something in which we can end up being absolute. We have to say that 70% of our effort or 50% of our effort

[Traduction]

de saccager une base de données informatisées, qui se trouve à Ottawa, depuis New-York ou depuis Bonn, en Allemagne de l'Ouest ou depuis Sydney en Australie, que de le faire depuis Ottawa. Mais la portée de toute loi que nous pourrions adopter ne dépasserait pas nos frontières. Quelle sorte de mesures le gouvernement du Canada devrait-il prendre pour faire face aux aspects internationaux des infractions relatives aux ordinateurs?

Prenons par exemple l'incident qui s'est produit à l'école Dalton. Même si une infraction avait eu lieu au Canada—ce qui ne semble pas être le cas—on peut se demander si oui ou non l'infraction peut donner lieu à l'extradition.

M. Ward: C'est une question intéressante. De nouveau, je ne pense pas qu'il y ait de réponse facile, monsieur Beatty. L'exemple que j'ai mentionné au début de mes observations, c'est un excellent exemple de ce genre de situation. La société de télécommunications a réussi à établir que l'infraction a eu lieu dans la région de San Francisco. Même si on avait réussi à identifier la personne, je tiens pour acquis qu'elle n'aurait été accusée que de l'utilisation illégale d'une installation de télécommunications aux États-Unis, c'est-à-dire le réseau de commutation de paquets et l'accès à ce réseau.

Si les États-Unis et le Canada voulaient collaborer dans ce domaine, je ne sais pas s'il existe d'autres cas où ce genre de collaboration serait nécessaire. J'essaie de penser aux genres d'infractions qui pourraient être commises aux États-Unis, par exemple, et dont les répercussions se feraient sentir au Canada. C'est comme si quelqu'un étendait le bras pour voler de l'argent de l'autre côté de la frontière. Je n'arrive pas à penser à d'autres cas semblables en ce moment, mais vous en connaissez peut-être. J'estime qu'il faudra trouver des arrangements multilatéraux avec les États-Unis pour faire face à ce problème.

Comme je l'ai dit plus tôt, si on essaie de régler tous ces problèmes dans le projet de loi, on pourra passer dix ans à le faire. Avec tout le respect que je dois au Sous-comité, je vous exhorterais d'élaborer un projet de loi relativement simple qui s'attaque aux cinq questions de base, disons, plutôt qu'à trois ou quatre questions vraiment épineuses. Je pense que la loi constituerait plus qu'un obstacle. Elle sensibiliserait beaucoup la population au problème, et d'autres mesures de contrôle seraient mises en place par la suite.

M. Beatty: Je pense que la loi aurait une incidence morale également: la société indiquerait aux personnes qui voulaient commettre un abus qu'elle considérerait qu'un tel acte est répréhensible.

M. Ward: Oui. C'est vrai. Je recommande que vous concentriez sur les cinq questions de base, d'abord plutôt que sur les autres, afin de trouver des solutions et de mettre en place des mesures de protection. Je suis convaincu qu'il n'existe pas de solution définitive à tous les problèmes. Il faut se mettre en tête que 70 p. 100 ou 50 p. 100 de nos efforts donneront lieu à 90 p. 100 des avantages et il faut se contenter

[Text]

potentially will reap 90% of the benefits, and stop at that point. To attempt to close the door completely, I think, would be totally impossible and impractical

• 1640

Mr. Beatty: You know, we do have access to compilations of various legislative initiatives in the U.S., but there seems to be relatively little work done in terms of pulling together examples of legislation in other jurisdictions. Has Peat, Marwick and Partners done any work in, for example, Europe or Japan? What sort of legislation is in place there to do with computer crime which might be useful to us?

Mr. Ward: We have not looked at computer legislation worldwide. We did look at computer abuse worldwide worldwide and did a survey, in fact, on a worldwide basis of our clients who had computer abuse problems—I mean both intentional and unintentional problems. Again, the vast majority of reported abuse was unintentional, accidental, controlled, problems. The most prevalent of them by the way, I may add, was the breakdown of physical security around the computer, as opposed to the data base not having the appropriate controls. But far and away, the largest problem was physical security. We did not extend that study I do not believe, and I could verify this, to what legislation was in place in those countries.

Mr. Beatty: What would be a good source for us to consult to try to get that information? It may very well be that a formula has been found in Sweden or Germany or Japan or the U.K. that would be applicable here.

Mr. Ward: It is very difficult offhand. I could certainly, on a personal basis, undertake that type of research in the next few weeks for the committee and at least get back with some basic comments from my partners around the world. One of our advantages at Peat, Marwick is to plug into 50 or so countries around the world relatively quickly and, if the committee so desired, I could attempt in the next two to three weeks before the end of May to inquire of my partners in at least the major countries around the world what legislation does exist. We may come up with absolutely nothing. But certainly I think we would get something in that vein, and I would be very pleased to do that for you, Mr. Beatty, if that would help out.

Mr. Beatty: I would appreciate that. It would be very helpful. There has been remarkably little written that I have found dealing with other jurisdictions.

There is one final area of interest. I came across terminology unfamiliar to me when I was doing some reading last night, and that is "time bombs" in software to try to protect software. Can you tell me what they are? How are they used? Who installs them? What types of software are they put into? What sort of implications are there in the installations of time bombs in software?

Mr. Ward: It sounds like something out of George Orwell, but I think what is being referred to is a situation where the person who develops the computer program builds in a particular routine. It may be based on a calendar date, for

[Translation]

de cela. Je pense qu'il serait tout à fait impossible et peu réaliste de chercher à résoudre tous les problèmes.

M. Beatty: Nous avons accès à des compilations de différentes initiatives législatives qui ont été prises aux États-Unis, mais il semble que très peu de travail a été fait pour regrouper toutes ces données. Est-ce que *Peat, Marwick and Partners* a fait du travail en Europe ou au Japon, par exemple? Quel genre de lois existent dans ces pays concernant les infractions relatives aux ordinateurs qui pourraient nous être utiles?

M. Ward: Nous n'avons pas examiné les lois qui existent au monde dans ce domaine. Nous avons fait une enquête sur nos clients qui avaient des problèmes d'utilisation abusive des ordinateurs à l'échelle mondiale. Je parle et des problèmes intentionnels et des problèmes non intentionnels. Je répète que la vaste majorité des cas d'abus qui sont signalés étaient non voulus, accidentels. Il s'agissait surtout de problèmes de sécurité physique, plutôt que d'un manque de protection de la base de données. Le plus grand problème était de loin celui de la sécurité physique. Je peux vérifier, mais je ne pense pas qu'on ait examiné les lois qui existaient dans ces pays.

M. Beatty: Où pourrait-on obtenir ces renseignements? Il se peut que la Suède, l'Allemagne, le Japon ou le Royaume-Uni aient trouvé une formule que nous pourrions utiliser ici.

M. Ward: Il m'est très difficile de vous répondre comme cela à pied levé. Je puis certainement m'engager personnellement à faire ce genre de recherches pour le Comité dans les quelques semaines à venir, et vous communiquer au moins les commentaires de base de mes associés partout au monde. L'un des avantages de *Peat, Marwick and Partners* est qu'on peut communiquer avec 50 pays assez rapidement. Si le Comité le veut, je peux essayer d'ici la fin de mai de demander à mes associés des principaux pays quelles lois existent dans leur pays. Il se peut qu'on ne trouve rien, mais je pense qu'il est plutôt probable qu'on trouve quelque chose. Si cela vous serait utile, monsieur Beatty, je serais heureux de le faire pour vous.

M. Beatty: Je vous en serais très reconnaissant. Cela nous serait très utile. Je n'ai pas réussi à trouver grand-chose d'écrit au sujet de la situation dans d'autres pays.

Je voudrais soulever un dernier point. J'ai trouvé un terme que je ne connaissais pas hier soir lors de mes lectures. Il s'agissait des «bombes à retardement» qui visent à protéger le logiciel. Pouvez-vous me dire de quoi il s'agit et comment on s'en sert? Qui est-ce qui les met en place? Dans quel genre de logiciels les incorpore-t-on? Quelles sont les implications de la mise en place de ces mécanismes à retardement dans un logiciel?

M. Ward: Cela a l'air de quelque chose que George Orwell aurait écrit. Je pense qu'on fait allusion à l'incorporation d'un sous-programme au programme d'ordinateur. Si, par exemple, un programme fait l'objet d'un accès une fois par semaine par

[Texte]

example, that if certain actions are not taken with that program—for example, the program is accessed once a week through a particular terminal—that software could corrupt itself and produce fallacious information for at least a period of time.

Mr. Beatty: I gather it may go further than that and cause computer crash, and be deliberately designed to do that.

Mr. Ward: That software may be then designed to go off into the rest of the computer and wreak havoc, if I can use that term. And that might—I use the word *might* . . . be used by a potential disgruntled employee who, if he believes he or she is going to be dismissed or whatever, could build that in and, if that person did not access the computer program within a predetermined period of time—let us say every week or every month—then the switch in the computer program would show ON. Not having been accessed for the last month, therefore, it could in effect say, I will initiate this special routine which goes throughout the computer.

Again, it sounds a little like something a mystery writer might write in a book on computer crime as opposed to reality. But there is some thought, I believe, that one of the apparent cases of computer crime has to do with a personnel or payroll program which was written by somebody who subsequently was dismissed, and when that person was not there, the program self-destructed or changed itself. Again, a program which would change itself probably would want to go back to a backup copy and use it again. But if that program then destroyed data or destroyed other parts of the computer, that would be a problem.

Mr. Beatty: The context in which I read the term was an article: "The Intricacies of Defusing the Software Time Bomb" by Dan Mersich who, apparently, is a Toronto lawyer. I guess the context in which he was using it was as a means for software vendors to protect the software; that is, if there was unauthorized copying of their software, or it was used in instances beyond the number of instances which was authorized for use by the vendor, that damage would be done to the data base of the individual institution that was using it in an unauthorized way. He was arguing that time bombs were very dangerous from the point of view of possible legal liabilities on the person who installed the time bomb in his own software to protect it.

• 1645

Are you aware of instances where this is being done to protect software?

Mr. Ward: I do not know of any situations. It seems akin to putting a time bomb in your car. If you do not access into the car properly, it blows up 10 minutes after the person drives off.

I can see what is happening, in that many people are concerned their software will be used elsewhere now, and they attempt to build in some degree of protection, maybe linked into the computer that it is actually sold to be used on. To take that one step further and actually put in some, what I would call negative impact computer program, i.e. something which

[Traduction]

l'entremise d'un terminal donné, et si cela ne se fait pas, le logiciel pourrait s'altérer et donner de fausses données pendant une certaine période de temps.

M. Beatty: Je crois savoir que ce mécanisme peut même aller plus loin et provoquer exprès l'arrêt de l'ordinateur.

M. Ward: On peut faire en sorte que le logiciel cause des ravages dans le reste de l'ordinateur, si je puis m'exprimer ainsi. Un employé mécontent pourrait . . . et je dis bien pourrait . . . incorporer un tel sous-programme au programme, s'il croyait qu'il allait être congédié, par exemple. Si le programme ne faisait pas l'objet d'un branchement dans une période de temps fixée à l'avance . . . disons toutes les semaines ou tous les mois . . . le bouton serait dans la position «ouvert». Si le programme n'avait pas fait l'objet d'un branchement depuis un mois, cela déclencherait le sous-programme spécial qui passerait dans tout l'ordinateur.

On dirait l'invention d'un auteur qui écrit de la fiction au sujet des infractions relatives aux ordinateurs. On pense que l'une des infractions de ce genre concerne un programme du personnel ou de la paye qui a été élaboré par un employé qui a été congédié par la suite. Lorsque l'employé n'était plus là, le programme s'est détruit ou s'est transformé. Un programme qui se transformerait chercherait probablement à avoir recours à une copie d'appoint. Mais il y aurait un problème si le programme détruisait des données ou d'autres parties de l'ordinateur.

M. Beatty: J'ai lu le terme dans un article de Dan Mersich qui, paraît-il, est avocat à Toronto. Son article s'intitule «*The Intricacies of Defusing the Software Time Bomb*». Je pense qu'il parlait de ce mécanisme en tant que mesure de protection pour les vendeurs de logiciel. Si une institution copiait un logiciel sans être autorisée à le faire, ou si elle s'en servait plus souvent que le vendeur ne l'a autorisée à le faire, la base des données de l'institution subirait des dommages. Il disait que ce mécanisme à retardement était très dangereux pour ce qui est des responsabilités juridiques possibles de la personne qui incorpore un mécanisme à retardement à son propre logiciel afin de le protéger.

Connaissez-vous des cas où on a recours à ce mécanisme pour protéger le logiciel?

M. Ward: Je ne connais pas de tels cas. C'est comme si on mettait une bombe à retardement dans votre voiture. Si on n'accède pas à la voiture comme il faut, elle explose dix minutes après.

Je comprends que beaucoup de personnes ont peur que leur logiciel soit utilisé ailleurs. Elles cherchent donc à incorporer au logiciel un mécanisme de protection, qui est peut-être lié à l'ordinateur sur lequel le logiciel est censé être utilisé. À mon avis, il n'est certainement pas souhaitable d'avoir ce genre de programme négatif, c'est-à-dire un programme qui va faire des

[Text]

will do damage, to my mind certainly is not something desirable, in the same way that wiring my car with a bomb to go off if somebody else drives away is also not desirable.

Mr. Beatty: Thank you very very much.

The Chairman: *Merci, monsieur Ward.*

Mr. Ward: Thank you very much, Madam Chairman.

The Chairman: Thank you for joining us. We will be waiting for the documentation on the legislation. It will be very much appreciated by us.

Mr. Ward: I will attempt to get that to the clerk of the committee in the next month or so.

The Chairman: Thank you. The meeting is adjourned to the call of the Chair.

[Translation]

dommages. De la même façon, il n'est pas souhaitable non plus que je mette une bombe à retardement dans ma voiture qui explosera si quelqu'un d'autre la prend.

M. Beatty: Merci beaucoup.

Le président: *Thank you, Mr. Ward.*

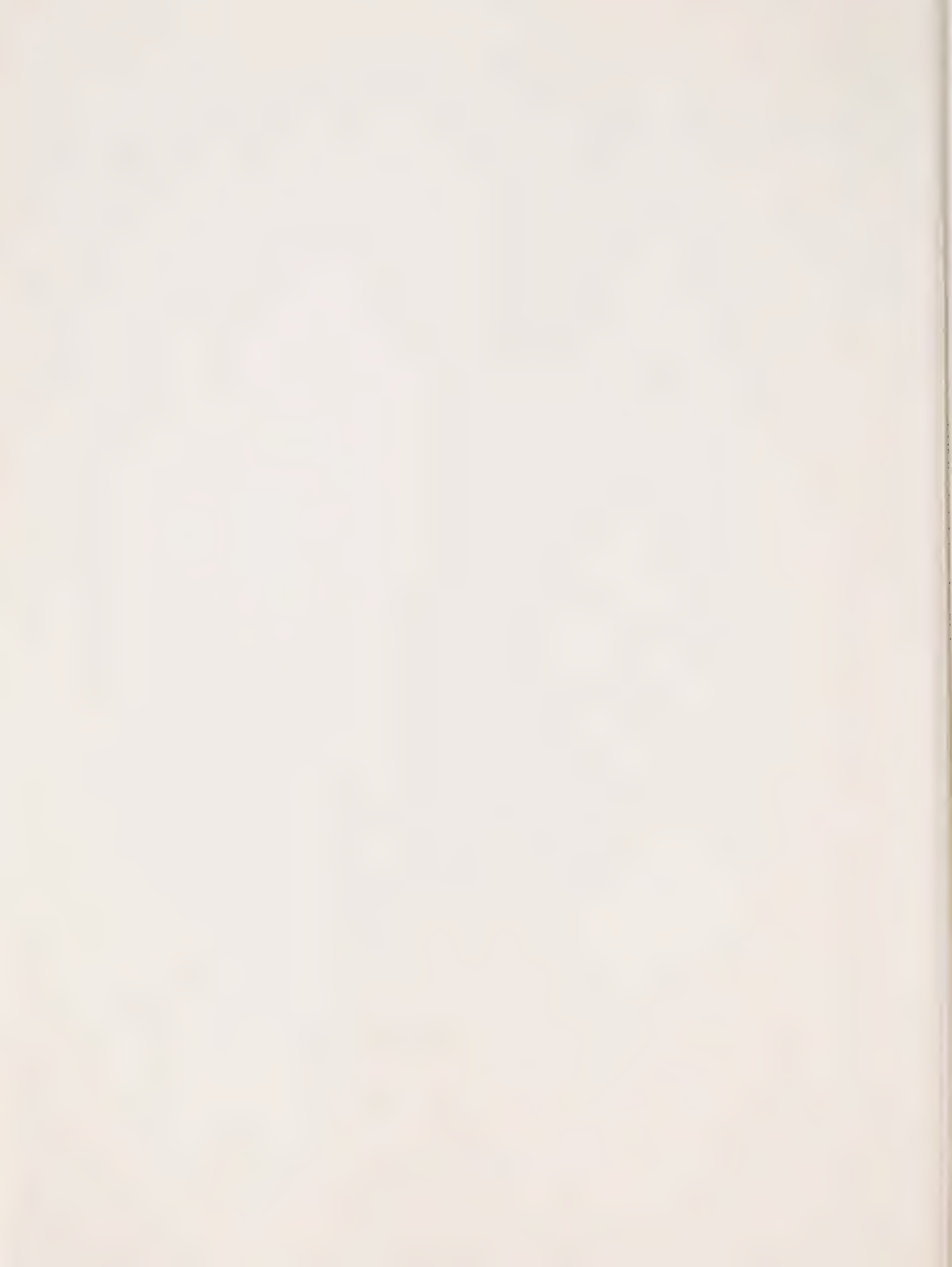
M. Ward: Merci beaucoup, madame le président.

Le président: Je vous remercie d'avoir comparu devant nous. Nous allons attendre les documents au sujet des lois qui existent ailleurs, et nous vous en remercions.

M. Ward: Je vais essayer d'envoyer ces documents au greffier dans un mois environ.

Le président: Merci. La séance est levée.







If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESSES—TÉMOINS

From Peat, Marwick and Partners:

Mr. Peter Ward

De «Peat, Marwick and Partners»:

M. Peter Ward

HOUSE OF COMMONS

Issue No. 5

Tuesday, May 3, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 5

Le mardi 3 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

TUESDAY, MAY 3, 1983

(7)

[Text]

The Sub-committee on computer crime met this day at 3:35 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-Committee present: Mrs. Céline Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From Western University: Professors John Palmer and David H. Flaherty, London, Ontario.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The Sub-committee agreed to proceed *in camera*.

At 4:05 o'clock p.m., the Sub-committee resumed its proceedings in public.

On motion of Mr. Robinson (*Etobicoke—Lakeshore*) it was agreed,—That, if the House consents, that the Sub-committee on computer crime be authorized to retain the services of Mr. Timothy Denton, lawyer and consultant as to act as an expert and advisor for the members of the Sub-committee on computer crime for a period not exceeding seven (7) weeks at a per diem rate of five hundred dollars (\$500), and that Mr. Denton be also assisted by Mr. Roger Voyer at a per diem rate of five hundred dollars (\$500) for a period not exceeding ten (10) days, and with Mr. Michael Dagg, at a per diem rate of three hundred dollars (\$300) for a period not exceeding twenty one (21) days.

The Sub-committee proceeded to consider a draft of its Second Report to the Standing Committee on Justice and Legal Affairs which is as follows:

In accordance with its Order of Reference of Tuesday, March 1st, 1983, respecting the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, your Sub-committee requests leave to be empowered to retain services of experts, and professional, technical and clerical staff as may be deemed necessary for the continuation of the consideration of its Order of Reference.

On motion of Mr. Robinson (*Etobicoke—Lakeshore*), it was agreed,—That the draft Report be the Second Report to the Standing Committee on Justice and Legal Affairs.

It was ordered,—That the Chairman report the Report to the Standing Committee on Justice and Legal Affairs.

Mr. Robinson (*Etobicoke—Lakeshore*) assumed the Chair.

The witnesses made statements and answered questions.

PROCÈS-VERBAL

LE MARDI 3 MAI 1983

(7)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h 35, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Céline Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, chercheuse, Service de la recherche, Bibliothèque du Parlement.

Témoins: De l'Université Western: Professeurs John Palmer et David H. Flaherty, London, Ontario.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars, 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Le Sous-Comité décide de siéger à huis clos.

À 16h 05, le Sous-comité reprend sa séance en public.

Sur motion de M. Robinson (*Etobicoke—Lakeshore*) il est convenu,—Que, si la Chambre l'autorise, que le Sous-comité sur les infractions relatives aux ordinateurs soit autorisé à retenir les services experts de M. Timothy Denton, avocat et expert-conseil, pour agir comme consultant et conseiller auprès des membres du Sous-comité pour une période n'excédant pas sept (7) semaines et à un taux per diem n'excédant pas cinq cents dollars (\$500), et que M. Denton soit assisté aussi de M. Roger Voyer à un taux per diem de cinq cents dollars (\$500), pour une période ne dépassant pas dix (10) jours et de M. Michael Dagg, à un taux per diem de trois cents dollars (\$300) pour une période ne dépassant pas vingt et un (21) jours.

Le Sous-comité procède à l'étude d'un projet du deuxième rapport au Comité permanent de la justice et des questions juridiques comme suit:

Conformément à son ordre de renvoi du mardi 1^{er} mars 1983, concernant l'étude du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions au droit de propriété relatifs aux ordinateurs, votre Sous-comité demande la permission pour qu'il soit habilité à retenir les services d'experts et aussi à employer le personnel professionnel et de soutien nécessaire afin de poursuivre l'étude de son ordre de renvoi.

Sur motion de M. Robinson (*Etobicoke—Lakeshore*), il est décidé,—Que le projet de rapport soit le deuxième rapport au Comité permanent de la justice et des questions juridiques.

Il est ordonné,—Que le président fasse rapport du rapport au Comité permanent de la Justice et des questions juridiques.

M. Robinson (*Etobicoke—Lakeshore*) assume la présidence.

Les témoins font des déclarations et répondent aux questions.

On motion of Mr. Beatty, it was ordered,—That the brief presented by Professor David H. Flaherty, intitled "Privacy Implications of Computer Crime" be printed as an appendix to this day's Minutes of Proceedings and Evidence. (*See Appendix "COMP-1"*)

At 5:39 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

Sur motion de M. Beatty, il est ordonné,—Que le mémoire présenté par le Professeur David H. Flaherty intitulé «*Privacy Implications of Computer Crime*», soit imprimé en appendice au procès-verbaux et témoignages de ce jour. (*Voir Appendice «COMP-1»*)

A 17h 39, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Tuesday, May 3, 1983

• 1603

The Chairman: I call the meeting to order.

The Subcommittee on Computer Crime has the honour to present its Second Report.

It is moved by Mr. Ken Robinson that the Second Report of the subcommittee on computer crime be concurred in. Is the motion adopted?

Mr. Beatty: Not concurred in, but rather that it be adopted. Concurrence is in the House.

Motion agreed to.

The Chairman: The last motion, which is moved by Mr. Robinson, is: That the chairperson report to the Standing Committee on Justice and Legal Affairs.

Motion agreed to.

The Chairman: Thank you for your patience. Now we are organized. If you will excuse me, I have to be in the House. I will give the Chair to Mr. Robinson. Thank you for coming.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): Our order of reference from the House of Commons is that the subcommittee resumes consideration of this order of reference respecting computer crime.

We have before us today two witnesses. The first witness is Professor John Palmer, from the University of Western Ontario, London, Ontario. Do you have a statement to present to us at this time, or do you wish just to make comments?

Mr. John Palmer (University of Western Ontario): I have a few opening remarks I would like to make, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): Fine. Thank you very much. Please continue.

Mr. Palmer: As you know from the work that has been circulated, I gather, my work has been on whether or not there should be enforceable property rights in computer software at all. In doing the work for Consumer and Corporate Affairs, I ran into a number of people throughout Canada and within the government who argued that there should be no property rights created especially for computer software, that there might be other techniques that could be used by people developing software to protect their software that might be more efficient for Canada.

If there were no defined property rights, some of these other ways of protecting investments might include such things as rapidly marketing their products before the imitators could capture a large section of the market. Another possibility might be to engage in something called price discrimination, namely charging those people who are more likely to make copies higher prices. A third possibility might be to use

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mardi 3 mai 1983

Le président: La séance est ouverte.

Le Sous-comité sur les infractions relatives aux ordinateurs a l'honneur de présenter son deuxième rapport.

Il est proposé par M. Ken Robinson que le deuxième rapport du sous-comité sur les infractions relatives aux ordinateurs soit approuvé. La motion est-elle adoptée?

M. Beatty: Pas approuvée, mais plutôt adoptée. L'approbation c'est à la Chambre.

La motion est adoptée.

Le président: La dernière motion proposée par M. Robinson est la suivante: Que le président fasse rapport au Comité permanent de la justice et des questions juridiques.

La motion est adoptée.

Le président: Merci de votre patience. Nous sommes maintenant organisés. Si vous voulez bien m'excuser, je dois me rendre à la Chambre. Je vais céder ma place à M. Robinson. Merci d'être venus.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Conformément à notre ordre de renvoi de la Chambre des communes, nous reprenons nos travaux sur les infractions relatives aux ordinateurs.

Nous accueillons aujourd'hui deux témoins. Le premier est M. John Palmer, professeur à l'université Western Ontario, de London. Avez-vous une déclaration à nous présenter en ce moment ou préférez-vous simplement faire quelques commentaires?

M. John Palmer (Université Western Ontario): J'ai quelques remarques liminaires à faire, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Merci beaucoup. Vous avez la parole.

M. Palmer: Comme vous avez pu le constater à partir du document qui vous a été distribué, mon travail a consisté à déterminer s'il devait exister des droits de propriété dans le domaine du logiciel. En effectuant mon travail pour le compte de Consommation et Corporations, j'ai rencontré un certain nombre de personnes au Canada et au sein de la Fonction publique qui estimaient qu'il ne fallait pas créer de droit de propriété spécialement pour le logiciel, que les concepteurs de logiciel pouvaient peut-être recourir à d'autres techniques plus efficaces pour le Canada pour protéger leurs produits.

En l'absence de droits de propriété bien définis, une façon de protéger les investissements dans le logiciel pourrait être de commercialiser rapidement le produit avant que les imitateurs ne puissent s'emparer d'une large part du marché. Un autre moyen consisterait peut-être à établir un barème de prix suivant lequel les personnes les plus susceptibles de copier le produit auraient à payer plus cher. Une troisième possibilité

[Text]

technological devices to protect their software. A fourth device would be to use trade secrecy in the common law.

All of these methods of protection, I decided in my study that I did for Consumer and Corporate Affairs, involve a lot of costs for the firms that develop software. In other words, they use resources that could be perhaps better used in other ways in society. And in some of these cases copyright protection, namely the legal creation of an intellectual property right in computer software, would help to reduce some of these costs and some of the waste of resources that might be used otherwise in rapid marketing, price discrimination, technological locks, or trade secrecy.

In the study that I did, of which I believe you have received a summary, I estimated that the magnitude of the saving to society from having copyright protection for computer software might be somewhere between \$20,000 and \$2 million a year. But these estimates were based primarily on studies of large substantial proprietary packages, and I would say that the data that I used are probably dated now; the study is already out of date because of the rapidly technologically changing area of computer software. Much of the work that people did four years ago was on giant computer software packages which were installed in numerous different establishments for large main-frame computers.

• 1610

Nowadays, it seems to me the major problem for computer software and the major problem of appropriation of property rights in computer software is with micro-computers and the silicon chips. These are problems of local clubs which are copying floppy discs of programs. And the question is one of, even if copyright is available for the software, how can it be enforced? And can it be enforced efficiently when there are small copiers who are copying \$200 worth of software and hence depriving developers of this software of some of the incentives to develop the software in the first place?

So the question I gather this subcommittee would like me to address is the question of whether extending the protection of that property right beyond the civil code, beyond just copyright protection, and including some clauses in the Criminal Code as well, might be appropriate in the area of computer software.

If I can briefly just talk a little bit about how an economist would approach that; we have a notion in economics that demand curves are downward sloping. In other words, any time we raise the price of any kind of activity, people will engage in that activity a little less.

One of the ways to raise the price of the activity of appropriating other peoples' software might be to increase the probability that people would be detected in appropriating other peoples' software, or to increase the punishment if they are detected and punished for appropriating that software. There are two possible ways of increasing this price and

[Translation]

serait d'utiliser des moyens techniques pour protéger le logiciel. Un quatrième moyen serait d'insérer une disposition dans la *common law* sur le secret commercial.

Toutes ces mesures de protection, comme j'en ai conclu dans l'étude que j'ai faite pour le compte de Consommation et Corporations, impliquent énormément de coûts pour l'entreprise qui crée du logiciel. En d'autres termes, ces mesures accaparent des ressources qui pourraient peut-être être plus utiles ailleurs dans la société. Et, dans certains cas, la protection du droit d'auteur, c'est-à-dire l'établissement légal d'un droit de propriété intellectuelle pour le logiciel, permettrait de réduire une partie de ces coûts et d'économiser des ressources qui pourraient servir à une mise en marché plus rapide, à l'établissement d'un barème de prix, à des dispositifs techniques de sécurité ou au secret commercial.

Dans l'étude que j'ai faite et dont vous avez reçu un résumé, j'estime que les économies que permettrait de réaliser un système de protection du droit d'auteur pour le logiciel s'élèveraient entre \$20,000 et \$2 millions par année. Mais cette estimation reposait principalement sur des études d'importants programmes produits de marques déposées, et je dirais que les données que j'ai utilisées sont probablement déjà périmées; l'étude est déjà dépassée à cause de l'évolution rapide de la technologie dans le logiciel. Une large part du travail qui a été fait il y a quatre ans portait sur des énormes ensembles de logiciels installés dans différents établissements pour de gros ordinateurs principaux.

Aujourd'hui, il me semble que le grand problème en ce qui concerne le logiciel et l'acquisition de droits de propriété tient aux micro-ordinateurs et aux microplaquettes de silicium. Ce sont des problèmes qui touchent les clubs locaux qui copient des programmes sur disquettes souples. Et la question est de savoir, même s'il y avait des droits d'auteur pour le logiciel, comment on les appliquerait? Et peut-on les appliquer de façon efficace lorsqu'il y a de petits copieurs qui reproduisent des logiciels de \$200 et qui découragent leurs auteurs d'en créer de nouveau?

Alors la question que le sous-comité aimerait que j'aborde est l'opportunité d'étendre la protection de ce droit de propriété au-delà du code civil, au-delà de la protection du simple droit d'auteur et d'inclure certaines dispositions également dans le code criminel.

Permettez-moi de vous exposer un peu comment un économiste aborderait la question. Il existe un principe d'économie selon lequel les courbes de la demande ont tendance à baisser. En d'autres termes, chaque fois qu'on relève le prix d'une activité, les gens s'y adonneront un peu moins.

L'une des façons de relever le prix de l'activité qui consiste à s'approprier du logiciel d'autrui serait d'augmenter la probabilité de dépistage des malfaiteurs, ou d'accroître la sanction relative à ces infractions. Il y a deux façons d'augmenter le prix et de dissuader davantage les malfaiteurs. La première

[Texte]

increasing the deterrence to this appropriation. One would be to increase the probability of detection, and one would be to increase the punishment.

Under copyright legislation alone, there are just damages, but copyright legislation could include punitive damages or maybe exemplary damages as well, which would mean there would be no need to include this particular appropriation of other peoples' property in the Criminal Code at all; it could be left within the Copyright Act, just in terms of increasing the punishments. There is not necessarily a strong argument for shifting part of that punishment into the Criminal Code. However, when it comes to the other possibility, namely, the possibility of increasing the probability of detection, increasing the probability that we will catch people who are appropriating other peoples' software, then there might be a stronger argument, because under the current arrangements of the Copyright Act, as I understand them, the only enforcement is private enforcement, as opposed to public enforcement of the act.

For instance, if I have written a program and I think that someone else is copying my program, I have to detect it and then I have to sue them for damages. Sometimes it may well be that if people are stealing a thousand dollars worth of software—and I use the word stealing in quotes because it is not clear that they are property rights yet—but if people are appropriating a thousand dollars worth of software it may not be worth my while to go through the civil procedures to recover damages, especially if I have to do it time and time again in terms of pursuing numerous people who might be copying my software without my permission.

In a situation like that, it might be advantageous to society to implement some form of criminal procedure as well, to amalgamate and take advantage of some of the cost savings of prosecuting people on a larger scale, or detecting some of the software rings that develop, in the sense of people who copy mass-produced software. But if that is the case for computer software, I want to ask one final question, in conclusion; that is, if there are these cost savings for computer software, in terms of having part of the detection put into the Criminal Code, why single that out from other forms of intellectual property? Why not have patent laws and all of copyright laws be generalized into the Criminal Code? I am not sure I would advocate that. In fact, I suspect that under pressure I would be forced to admit that I would not advocate that. I then begin to wonder what makes computer software so special that it should be included in the Criminal Code and none of the other forms of intellectual property should be.

Thank you very much, Mr. Chairman.

• 1615

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you very much for your remarks.

Mr. Beatty, do you wish to question first, or do you want me to lead off?

Mr. Beatty: Why do you not go ahead and I . . .

[Traduction]

serait d'accroître la probabilité de dépistage, la seconde d'établir des sanctions plus sévères.

Aux termes de la Loi sur le droit d'auteur, on ne prévoit que des dommages-intérêts, mais la loi pourrait comprendre des dommages-intérêts punitifs ou peut-être des dommages-intérêts exemplaires, ce qui éviterait de devoir inclure cette forme particulière d'acquisition du bien d'autrui dans le code criminel, simplement en établissant des peines plus sévères. La prévision de cette sanction dans le code pénal ne trouve pas de grandes justifications. L'autre possibilité, cependant, celle d'accroître la probabilité de dépistage des personnes qui s'approprient du logiciel d'autrui, a davantage sa raison d'être; parce que selon les dispositions actuelles de la Loi sur le droit d'auteur, si je comprends bien, c'est au secteur privé que revient l'application de la loi et non au secteur public.

Par exemple, si j'ai créé un programme et que j'ai l'impression que quelqu'un le copie, je dois trouver le coupable et tenter des poursuites en dommages et intérêts. Parfois, il se pourrait très bien que si quelqu'un vole pour un millier de dollars de logiciel—et j'emploie le mot «vole» entre guillemets parce qu'on ne sait toujours pas s'il s'agit de droits de propriété—mais si quelqu'un s'approprie un millier de dollars de logiciel, cela ne vaut peut-être pas la peine que j'intente des poursuites au civil en dommages et intérêts, spécialement si je dois souvent poursuivre de nombreuses personnes qui copient mon logiciel sans mon autorisation.

Dans une telle situation, la société aurait peut-être avantage à établir une procédure judiciaire quelconque qui permettrait de tirer quelque profit des économies réalisées en intentant des poursuites sur une grande échelle ou en mettant au jour des réseaux de vol ou de sirotage de logiciels. Mais si c'est le cas pour le logiciel, j'ai une dernière question à poser pour terminer: s'il y a des économies à réaliser pour le logiciel en insérant des dispositions de dépistage des infractions dans le code pénal, pourquoi différencier les logiciels d'autres formes de propriété intellectuelle? Pourquoi les lois sur les brevets et toutes les lois sur le droit d'auteur ne seraient-elles pas insérées dans le Code criminel? Je ne suis pas sûr que je préconiserais cette solution. En fait, si on me le demandait, je pense que je ne préconiserais pas cette solution. Je commence alors à me demander en quoi le logiciel d'ordinateur est-il si spécial pour qu'on veuille l'inclure dans le Code criminel, contrairement à toute autre forme de propriété intellectuelle.

Merci beaucoup, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci beaucoup pour vos observations.

Monsieur Beatty, voulez-vous poser la première question, ou voulez-vous que je commence?

M. Beatty: Pourquoi ne commencez-vous pas?

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Professor Palmer, you indicated that you had provided a report and that that report is now out of date. Do you contemplate updating that report that you did some, what, a few months ago, I guess.

Mr. Palmer: The paper that I sent to you . . . is this the one you are talking about, or are you talking about . . .

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): The one that you did for Consumer and Corporate Affairs.

Mr. Palmer: The one I did for Consumer and Corporate Affairs, this monograph I completed about three years ago. It was just published, I guess about eight or nine months ago, though; it takes quite a while.

I sent you a paper that was an abbreviated version of this, which was recently presented at a conference.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): But is it an updated paper?

Mr. Palmer: It is slightly updated. It mentions the problems of micro-computers and computer software for micros, but it does not deal specifically with them, no.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Are you contemplating updating the report?

Mr. Palmer: Not at this time, no.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Not at this time. Can you tell us the general areas where the updating should be carried out in your report, so that when we are looking at the report and your most recent paper you have provided the committee with, we have some indication of the areas that you consider should be updated.

Mr. Palmer: I think the major area that is important now is to give an idea of the size of the micro-computer software area, and if possible to get some evidence about how much appropriation of software from micro-computers goes on. I mean, I hear apocryphal stories, anecdotal stories. I am sure you have heard evidence about them as well from other witnesses. I have no idea how much of that goes on.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You made the statement that if copyright is available, how can it be enforced? What are your suggestions in this regard?

Mr. Palmer: In general, I would say the private enforcement works reasonably well; that people who lose, because of the appropriation of other peoples' software, know that they have lost, and they generally have a good idea who is doing the appropriating. They might lack some subpoena power to get the data or the evidence that they need to sue the appropriator for damages, and there may be sufficiently low probability of success that they do not take the chances that they would need. In that case it might be reasonable to incorporate some punitive damages into the Copyright Act, or some exemplary damages into the Copyright Act, but still to leave it in the hands of private enforcement, because those are the people

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Palmer, vous avez dit que vous avez présenté un rapport et que ce rapport était maintenant désuet. Comptez-vous mettre à jour ce rapport que vous avez rédigé il y a quelques mois à peine?

M. Palmer: Le document que je vous ai envoyé . . . Est-ce de celui-ci que vous parlez ou . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Le rapport que vous avez fait pour Consommation et Corporation.

M. Palmer: Cette monographie que j'ai écrite pour Consommation et Corporations a été faite il y a environ trois ans. Mais elle vient d'être publiée il y a 8 ou 9 mois, cela prend du temps.

Je vous ai envoyé une version abrégée de ce rapport qui a été présenté dernièrement à une conférence.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ce document a-t-il été mis à jour?

M. Palmer: En partie. Il fait état des problèmes des micro-ordinateurs et du logiciel d'informatique destiné aux micro-ordinateurs, mais il n'en traite pas en profondeur.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Comptez-vous faire une mise à jour du rapport?

M. Palmer: Pas en ce moment, non.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Pas pour le moment. Pouvez-vous nous dire en général sur quoi devrait porter la mise à jour de votre rapport, pour que nous ayons une idée des questions doivent être mises à jour, lorsque nous étudierons le rapport et le tout dernier document que vous avez présenté au comité?

M. Palmer: Je pense que ce qui est le plus important maintenant, c'est de vous donner un aperçu de l'envergure du logiciel pour micro-ordinateurs et, si possible, de tenter de déterminer l'ampleur du problème relié à l'appropriation de ce logiciel. J'entends toutes sortes d'histoires à ce sujet. Je suis sûr que d'autres témoins vous en ont raconté de toutes sortes. Je n'ai aucune idée de l'ampleur du problème.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé de l'application du droit d'auteur dans ce domaine. Quelles sont vos suggestions à cet égard?

M. Palmer: En général, je dirais que l'application par le secteur privé est relativement efficace; que les personnes qui subissent des pertes par suite de l'acquisition illégale de logiciels savent qu'elles sont victimes et ont généralement une bonne idée de l'identité des malfaiteurs. Elles n'ont peut-être pas le pouvoir voulu pour exiger les données et établir la preuve dont elles ont besoin pour tenter des poursuites en dommages et intérêts contre les malfaiteurs, et les probabilités de réussite sont peut-être trop faibles pour qu'elles se donnent la peine de poursuivre. Dans ces circonstances, il conviendrait peut-être d'incorporer des dommages-intérêts punitifs ou exemplaires dans la Loi sur le droit d'auteur, en laissant toutefois l'application de la loi entre les mains du secteur privé,

[Texte]

who know when they have a loss and they generally know who is causing the loss.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you feel that the victim should have some responsibility here to disclose the computer crime? I suppose if it were in the Criminal Code it would be incumbent upon the individual to make known that a crime had taken place, but if it is just under the Copyright Act, I suppose there is not the same onus on the individual to disclose the crime. What do you have to say about that?

Mr. Palmer: I had not contemplated that issue, and I do not see that it would make a lot of difference from the point of view of enforcement of the property rights.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you not think there should be an obligation on the victim to make disclosure?

Mr. Palmer: I am not sure that I see any benefits to society from requiring disclosure. The victim would have to make some disclosure of some sort if he were to sue for damages, I presume. Would that not be public disclosure? It seems to me that is a sufficient kind of disclosure.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, certainly, if you sue for damages there is a form of disclosure, that is true. But if you are not suing for damages, but merely assisting in the laying of an information under some section of the Criminal Code, or for some other action to be taken, albeit there might be, I suppose, a judgment for restitution of some kind in damages, I am just wondering if you feel there should be some requirement by the individuals involved in computers to report any so-called computer theft, computer abuse.

• 1620

Mr. Palmer: From the standpoint of the research I have done so far, Mr. Chairman, I see no reason for that. There might be other reasons outside my area of expertise, but I see no reason for it.

The Acting Chairman (Mr. Robinson (Etobicoke... —Lakeshore)): What you have suggested is that if you increase the probability of detection, I suppose you are considering by that there will be some sophisticated ways of protecting the computer and the software and...

Mr. Palmer: I had in mind, actually, not so much sophisticated techniques, but also the provision of publicly funded sections of law enforcement agencies to aid in the detection of this. That might be one of the benefits that people might see coming from putting computer crime into the Criminal Code.

The Acting Chairman (Mr. Robinson (Etobicoke... —Lakeshore)): But how do you see this as a deterrent? I think you link deterrence with two statements you made—increasing the probability of detection, and increasing the punishment; you link them both, however, to deterrence. How do you see the first as having anything to do with deterrence?

[Traduction]

parce qu'on sait généralement qui a commis le méfait lorsqu'on subit une perte.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Pensez-vous que la victime devrait être tenue de signaler les infractions reliées à l'informatique? S'il y avait des dispositions à cet égard dans le Code criminel, il incomberait à la victime de signaler toute infraction, mais aux termes de la Loi sur le droit d'auteur, cette responsabilité de signaler les infractions n'est pas aussi explicite. Quels sont vos commentaires là-dessus?

M. Palmer: Je n'avais pas pensé à cet aspect de la chose, et je ne crois pas que cela fasse tellement de différence du point de vue de l'application des droits de propriété.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Pensez-vous que la victime devrait être obligée de signaler les infractions dont elle est victime?

M. Palmer: Je ne vois pas ce que cela donnerait de plus. Je suppose que la victime serait obligée de signaler une infraction si elle intentait des poursuites en dommages et intérêts. Cela me semble suffisant.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il est évident que si vous intétez des poursuites en dommages et intérêts, une infraction aura été signalée. S'il n'y a pas de poursuite pour dommages et intérêts, mais «dénunciation» aux termes d'un article du Code criminel, ou toute autre procédure judiciaire, ordonnance de restitution de quelque sorte pour dommages causés, pensez-vous qu'il faudrait obliger ceux qui travaillent dans le domaine de l'informatique à signaler les cas de vols ou d'utilisation abusive de matériel informatique?

M. Palmer: D'après les recherches que j'ai faites jusqu'à présent, monsieur le président, je ne crois pas que ce soit nécessaire. Il y aurait peut-être des justifications dans d'autres domaines, mais pas dans le mien.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé d'accroître la probabilité de dépistage; cela doit vouloir dire qu'il y aurait des moyens perfectionnés de protéger l'ordinateur et le logiciel et que...

M. Palmer: Ce à quoi je pensais, en fait, ce n'est pas tellement à des techniques sophistiquées, mais plutôt à des organismes publics chargés du dépistage de ces infractions. C'est peut-être l'un des avantages que comporterait l'insertion de dispositions relatives au crime informatique dans le Code criminel.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais comment cela aurait-il un effet de dissuasion? Je pense que vous établissez un rapport entre la dissuasion d'une part et le fait d'accroître la probabilité de dépistage et d'imposer des peines plus sévères d'autre part. Qu'est-ce que le premier élément a à voir avec la dissuasion?

[Text]

Mr. Palmer: If we increase the probability that someone will be detected in appropriating someone else's software, that means the expected costs to them of appropriating that software goes up and they will have less of an incentive to appropriate the software.

For example, if I can put this in terms of an example, if a person were to contemplate appropriating a software package that is worth let us say \$2,000 for a micro-computer—that would be a very expensive software package—with about a 0.5% chance of being caught, and the expected punishment of only \$2,000 if they do get caught, then there is very little to deter them from appropriating that software package, copying it off a friend's disc, or something like that.

Alternatively, if there is a higher probability that they are going to be caught, that means the expected punishment they would have to bear if they do get caught would go up. And if that were coupled with higher punishments if they were caught, such as punitive damages or exemplary damages of some sort, that would even more greatly increase the expected costs of appropriating someone else's property rights.

What I have talked about is something that economists call economic analysis of crime. It deals with both the probability of being caught and the size of the punishment. When you multiply the two together, you get the expected cost of committing the crime.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): So you are talking really about damages, and exemplary damages as well.

Mr. Palmer: Yes; those go under the punishment side, as opposed to the probability side.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): What about the suggestion that the Criminal Code could be amended in some way? You apparently do not particularly favour that approach. Do you not feel that if you want to detect so-called computer crime, for lack of a better term, you would have much wider and greater powers under the Criminal Code to do this than you would have just under the ordinary copyright statute?

Mr. Palmer: That is what I was trying to say, yes—that in the sense of increasing the probability of detecting this, all of the powers of the law enforcement agencies would be available to detect and help convict people who engage in appropriating other peoples' property.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): Have you considered how this might be done by way of an amendment to the Criminal Code?

Mr. Palmer: I have not.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have not.

Now, you also mentioned that at this time the software or the technology, call it what you like, is not considered as intellectual property, as such. What would you propose by way of definition in order to see to it that it becomes intellectual

[Translation]

M. Palmer: S'il est plus probable qu'une personne se fasse prendre à s'approprier du logiciel de quelqu'un d'autre, cela veut dire que les risques ou «coûts» d'acquisition de ce logiciel augmentent et, en conséquence, la personne sera moins portée à s'en approprier.

Prenons un exemple: si une personne envisage de s'approprier un logiciel d'une valeur de \$2,000 pour un micro-ordinateur—ce qui est très cher pour un logiciel—alors qu'il n'y a que 0.5 p. 100 de chance de se faire prendre et que la peine prévue est de \$2,000 seulement, il y a là très peu pour la dissuader de s'approprier du logiciel, de le reproduire d'une façon quelconque.

Par contre, si les chances de se faire prendre sont plus fortes, cela veut dire que la peine à laquelle on s'expose serait plus sévère. Et si tout cela était assorti à des peines plus sévères comme les dommages punitifs ou exemplaires, les coûts inhérents à l'appropriation des droits de propriété d'autrui seraient encore plus élevés.

Ce dont je viens de vous parler, les économistes appellent cela une analyse économique du crime. Cela porte sur la probabilité de se faire prendre et sur la sévérité de la peine. Quand vous multipliez les deux, vous obtenez le coût inhérent à la perpétration du crime.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Alors, vous parlez vraiment de dommages-intérêts punitifs.

M. Palmer: Oui, ce sont des éléments de la peine, par opposition à la probabilité de dépistage.

Le président suppléant (M. Robison (Etobicoke—Lakeshore)): Que pensez-vous d'amendements au Code criminel? Vous ne semblez pas particulièrement favorable à cette solution. Ne pensez-vous pas que le Code criminel, par opposition à la Loi ordinaire sur le droit d'auteur, serait beaucoup plus efficace pour dépister ce qu'on appelle, à défaut de mieux, le crime informatique?

M. Palmer: Oui, c'est ce que j'essayais de vous dire: pour accroître la probabilité de dépistage du crime, tous les pouvoirs des services d'application de la loi seraient en place pour dépister et aider à condamner les personnes qui s'approprient du bien d'autrui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Avez-vous songé au genre d'amendement qu'on pourrait apporter au Code criminel pour en arriver à ce résultat?

M. Palmer: Non.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous n'y avez pas songé.

Vous avez également dit qu'à l'heure actuelle le logiciel ou la technologie, qu'on l'appelle comme on voudra, n'est pas considéré comme une propriété intellectuelle comme telle. Que proposeriez-vous comme définition pour que cela devienne une

[Texte]

property, or a kind of intellectual property—like property trademarks, and so on?

Mr. Palmer: Let me back off from the initial statement a bit. My understanding is, from talking with lawyers about current cases, that computer software . . . there has not been a case that has actually gotten through the courts testing whether computer software is copyrightable. There is a good chance that it is; there have been a number of injunctions, including Anton Pillar injunctions, which have suggested that computer software is copyrightable. If that is the case, then there is no problem. However, I would hope that in the forthcoming amendments to the Copyright Act, which I gather are about to be presented sometime within the next six months, there would be explicit recognition of computer software in the Copyright Act, to make explicit the recognition of the intellectual property right in computer software.

• 1625

The Acting Chairman (Mr. Robinson (Étobicoque—Lakeshore)): If it is not a property then what is it at the present time?

Mr. Palmer: If it is not property I have no idea what it is. That is a good question. It is the result of someone's investment. I think of it as a property. I am sure that you do too, based on your questioning.

The Acting Chairman (Mr. Robinson (Étobicoque—Lakeshore)): How do we deal with it other than . . . as you say, if you are using the term, stealing something that is not property, you put the word stealing in quotation marks . . . you know, we cannot continually do that. How do we actually describe what we are talking about or what we are dealing with?

Mr. Palmer: I should think that talking about it in terms of computer software which has been developed by various people would be the way to talk about it. I would think of it as a property, but that is because I have recommended it be included in intellectual property rights.

The Acting Chairman (Mr. Robinson (Étobicoque—Lakeshore)): We have been talking about computer software, but would the same thing apply to a firmware or hardware, or whatever other term . . . ?

Mr. Palmer: Certainly, certainly. Hardware is another story; but certainly firmware. Anything that has been the result of the development of something that is sort of a mental process and the expression of an idea. It is something like the analogies to phonograph records at the turn of the century, incorporating on some new medium that people thought was a new fad; the creative efforts of composers . . . You know, we have a new medium, these silicon chips, that plug into computers, and it seems to me the same kind of analogy could be used . . . that they should be . . . but hardware is another story.

The Acting Chairman (Mr. Robinson (Étobicoque—Lakeshore)): It seems rather easy to consider that when you are talking about firmware you are talking about something

[Traduction]

propriété intellectuelle, ou un genre de propriété intellectuelle comme les marques de commerce, et ainsi de suite?

M. Palmer: J'aimerais revenir un peu sur ce que j'ai dit. D'après mes discussions avec des juristes au sujet de causes actuellement en litige, je ne crois pas qu'il ait déjà été établi par les tribunaux que le logiciel d'ordinateur puisse faire l'objet d'un droit d'auteur. Il y a de bonnes chances que ce soit possible, il y a eu un certain nombre d'injonctions, celles d'Anton Pillar notamment, qui portent à croire que le logiciel peut faire l'objet d'un droit d'auteur. Si c'est le cas, il n'y a pas de problème. Cependant, j'espère que dans les prochains amendements à la Loi sur le droit d'auteur qui doivent être présentés, je crois d'ici environ six mois, on reconnaîtra explicitement le logiciel en tant que droit de propriété intellectuelle.

Le président suppléant (M. Robinson (Étobicoque—Lakeshore)): Mais si ce n'est pas une propriété aujourd'hui, qu'est-ce que c'est?

M. Palmer: Si ce n'est pas une propriété, je ne sais pas ce que c'est. C'est une bonne question. C'est le résultat d'un investissement effectué par quelqu'un. Pour moi c'est une propriété et je pense que pour vous aussi, à en juger d'après vos questions.

Le président suppléant (M. Robinson (Étobicoque—Lakeshore)): Mais que pouvons-nous faire d'autre que . . . Peut-on utiliser le terme de vol si ce n'est pas la propriété de quelqu'un?. On ne peut pas toujours mettre le mot entre guillemets. Comment donc décrire ce dont il s'agit dans la réalité?

M. Palmer: Je pense qu'il faut décrire cela comme un logiciel informatique mis au point par diverses personnes. À mes yeux, cela est une propriété et c'est pourquoi j'ai recommandé de l'inclure dans les droits de propriété intellectuelle.

Le président suppléant (M. Robinson (Étobicoque—Lakeshore)): Nous parlons ici de logiciel informatique, mais la même chose s'appliquerait-elle au matériel informatique ou au logiciel fixe . . . ?

M. Palmer: Certainement, oui. Le matériel est différent mais cela s'appliquerait certainement au logiciel fixe. Tout ce qui résulte d'un processus mental et qui consiste en l'expression d'une idée . . . Si vous voulez, on peut prendre comme analogie les disques de phonographe au début du siècle où l'on inscrivait sur un support nouveau les efforts créatifs des compositeurs . . . Nous aussi avons aujourd'hui un support nouveau, les puces de silicium que l'on branche sur un ordinateur, et il me semble qu'on peut utiliser la même analogie . . . Mais le matériel est une autre histoire.

Le président suppléant (M. Robinson (Étobicoque—Lakeshore)): Il est assez facile, dans le cas du logiciel fixe, de

[Text]

that is a piece of property. It is something you can perceive and see.

Mr. Palmer: I am sorry to interrupt you; the problem is that the piece of property is worth about five dollars in terms of the materials and what it costs to make it. The property is what is embedded in that piece of material, just as the property on a phonograph record that is 49¢ worth of plastic is not the plastic. The property is what is embedded in it or transcribed onto it. It is the same with the chips. The property value is what is embedded in the chip or what is transcribed onto the chip. It is a kind of intellectual property, and this is just a medium for the expression of this intellectual property.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): My last question to you, and then I will turn it over to Mr. Beatty... You indicated that a change in the Intellectual Property Act or laws would be helpful. I do not think we have changed our Copyright Act in 50 years in Canada.

Mr. Palmer: I think it is closer to 60.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): Is it closer to 60? Well, you are more familiar with it than I am, but I seem to recall when I inquired about it that it has been a long time since there has been any change. If we are waiting for a change in the copyright law, we might wait a long time. Certainly this is a problem that cannot wait another 50 or 60 years.

My last question to you then is: How do you see that we should go about getting the quickest response to this problem as perceived today?

Mr. Palmer: I would say that looking for the quickest response might be a mistake, because we might be embedding something in the Criminal Code that belongs in the civil code. It seems to me quite likely, based on the judgments I have heard on injunctive relief in terms of copyright protection of software, that the courts will be interpreting the current Copyright Act as being something which includes computer software whether it is going to be explicitly included or not. And so, it may well be that, rather than include this one form of intellectual property in the Criminal Code and leaving all the others out there with laws that are just about as arcane as the Copyright Act, we might be better to leave it up to the judicial interpretation to re-interpret the Copyright Act while we are waiting for it to be made explicit, rather than to make the massive leap from the civil code to the Criminal Code.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): Thank you, Professor Palmer.

Mr. Beatty, do you have some questions?

Mr. Beatty: I must make the confession at the outset Professor Palmer: I was sufficiently at sea when I was trying to grasp the technological and legal aspects of my own bill, even before we injected econometric models and questioned the Copyright Act, both of which are immensely complex. I hope you will bear with me if my questions betray my ignorance.

[Translation]

décéder qu'il s'agit là d'une propriété car c'est quelque chose que l'on peut voir et toucher.

M. Palmer: Excusez-moi de vous interrompre. Le problème est que ce bien, sur le plan matériel, coûte 5 dollars à produire. La propriété est plutôt ce qui est inscrit dans ce support matériel, de la même façon que la propriété dans le cas d'un disque de phonographe ne se limite pas au 49c. de plastique qui compose le disque. C'est ce qui y a été enregistré ou transcrit qui représente la valeur. C'est la même chose avec les puces. La valeur est représentée par ce qui est inscrit dans la puce, c'est-à-dire qu'il s'agit d'une propriété intellectuelle et non pas de la possession du support matériel qui, lui, ne sert qu'à l'expression de cette propriété intellectuelle.

Le président suppléant (M. Robinson (Étobicoke—Lakeshore)): Dernière question avant de donner la parole à M. Beatty... Vous avez dit qu'une modification de la législation régissant la propriété intellectuelle serait utile. Je ne pense pas que nous ayons touché à notre Loi sur le droit d'auteur depuis 50 ans.

M. Palmer: Plutôt depuis 60 ans.

Le président suppléant (M. Robinson (Étobicoke—Lakeshore)): Plutôt 60 ans? Vous connaissez mieux la question que moi, mais je sais de toute façon que cela fait bien longtemps que l'on n'y a pas touché. Il faut attendre une modification de la Loi sur le droit d'auteur, cela risque d'être long. Ce problème-là en tout cas ne pourra attendre encore 50 ou 60 ans de plus.

Je vous pose donc la question suivante: quel serait le moyen le plus rapide de résoudre ce problème tel qu'il se présente aujourd'hui?

M. Palmer: Ce serait peut-être une erreur de rechercher la solution la plus rapide car nous risquons d'inscrire des dispositions dans le Code criminel qui devraient plutôt figurer dans le Code civil. J'ai l'impression, selon les précédents créés par les tribunaux relativement à des demandes d'injonctions visant la protection du droit d'auteur de logiciel, que la jurisprudence va interpréter la Loi sur le droit d'auteur actuel comme applicable au logiciel informatique, que cela soit dit explicitement ou non dans la loi. Il se pourrait donc bien, plutôt que d'inclure cette seule forme de propriété intellectuelle dans le code pénal et de confiner toutes les autres formes dans des lois qui sont à peu près aussi archaïques que celle du droit d'auteur, qu'il vaudrait mieux s'en remettre aux tribunaux afin qu'ils réinterprètent la Loi sur le droit d'auteur plutôt que de faire le grand saut du code civil au code criminel.

Le président suppléant (M. Robinson (Étobicoke—Lakeshore)): Je vous remercie, professeur Palmer.

Monsieur Beatty, avez-vous des questions?

M. Beatty: Je dois commencer par un aveu, professeur Palmer: j'ai déjà eu beaucoup de mal à saisir les applications technologiques et juridiques de mon propre projet de loi avant de me lancer dans des considérations économétriques et une remise en question de la Loi sur le droit d'auteur qui sont tous deux des sujets extraordinairement complexes. J'espère que

[Texte]

Could I get some guidance from you as to . . . when you are talking about software, what are you really talking about? If you are talking about a computer program, my understanding would be that you are talking about instructions that are given to a computer to process information in a particular way.

• 1630

Assuming that you are copyrighting those instructions, what other instructions for machinery could you copyright? Can you give me an example of something other than computer software and computer programs that is in the form of instructions that one might copyright?

Mr. Palmer: Any kind of instruction manual; the auto repair manuals would be a good example. A set of instructions; any set of instructions.

Mr. Beatty: What you are copyrighting there is the particular form that the information appears in, but not the ideas that are contained therein.

Mr. Palmer: That is exactly right. Let us take a good current case in the United Kingdom. If you develop a computer game that has frogs jumping across rivers, for example, if someone else takes the game apart, backs the information off the chip onto a disc, and then starts manufacturing their own chips—in other words they are slavishly copying, that is the jargon my friends in the law school use, that chip—I would say that is probably an infringement of copyright and should not be allowed.

However, if someone looks at that and says that is an interesting idea, having frogs jump across a river and trying to eat ladybugs along the way—or whatever it is they do in this game—I think I would like to develop a similar type of game, and then develops his own game through his own independent effort, and without slavishly copying, then essentially all he has done is use the idea, adapt the idea.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You mean he put in a toad instead of a frog.

Mr. Palmer: A toad, a frog—but he did not steal their game; he did not slavishly copy the game. If I borrow the idea, use the idea, adapt the idea, then it is less likely to be an infringement of copyright. And that is generally true with most forms of copyright. If you write a book on bicycle repair, I can use the ideas from your book as long as I do not copy. I mean, I can essentially use the algorithm in terms of computer software. I can use the algorithm as long as I do not copy the words. I can have the same outline for my book.

Mr. Beatty: That is precisely the point, the algorithm. Assume that you had a program for word processing, for example, for an Apple 3. In your extract you talked about one way of detecting abuse of copyright being to put phony or irrelevant lines into the program, and if that is copied then it

[Traduction]

vous ne m'en voudrez pas si mes questions trahissent mon ignorance.

Pourriez-vous me dire . . . lorsque vous parlez de logiciel, de quoi s'agit-il exactement? Si vous parlez d'un programme informatique, j'imagine qu'il s'agit là d'un ensemble d'instructions que l'on donne à un ordinateur en vue de traiter les données d'une certaine façon.

En supposant que l'on décrète un droit d'auteur sur ces instructions, quelles autres instructions de machines pourraient être dans le même cas? Pourriez-vous nous donner un exemple, autre que le logiciel informatique et les programmes d'ordinateur, qui pourrait être protégé par le droit d'auteur?

M. Palmer: N'importe quel manuel d'instruction; un bon exemple serait les manuels de réparation d'automobile. N'importe quel ensemble d'instructions.

M. Beatty: Ce qui est protégé ici, c'est la forme particulière que revêt l'information, mais non pas les idées qui y sont contenues.

M. Palmer: Exactement. Prenons un bon exemple récemment survenu au Royaume-Uni. Si vous mettez au point un jeu électronique dans lequel des grenouilles sautent par dessus une rivière et que quelqu'un démonte la cassette et copie sur un disque les données contenues dans la puce, il se met ensuite à produire ses propres puces—c'est-à-dire qu'il ne fait que copier servilement cette puce comme le disent mes amis juristes—ce serait-là un empiètement sur le droit d'auteur qu'il faudrait interdire.

Par contre, si quelqu'un prend ce jeu et se dit que c'est une idée intéressante que de faire sauter une grenouille par dessus une rivière et d'avalier des coccinelles en chemin, et conçoit un jeu similaire par un travail indépendant et qui n'est pas une copie servile du premier, alors il s'est seulement servi de l'idée pour l'adapter.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Est-ce qu'il suffirait qu'il prenne un crapaud à la place d'une grenouille?

M. Palmer: Un crapaud, une grenouille; ce qui compte, c'est qu'il n'a pas volé le jeu, il ne l'a pas copié servilement. Si j'emprunte une idée et que je l'adapte, il y a beaucoup moins de chance que je commette un empiètement. C'est généralement vrai de la plupart des formes de propriété intellectuelles. Si vous rédigez un manuel sur la réparation des bicyclettes, je peux emprunter les idées qui figurent dans votre livre à condition de ne pas le copier. Autrement dit, en informatique, je peux utiliser les mêmes algorithmes que vous à condition que je ne copie pas les mots. Je peux suivre dans mon livre la même démarche que vous.

M. Beatty: C'est exactement cela. Supposons que vous ayez un programme de traitement de texte pour un ordinateur Apple 3, par exemple. Vous avez dit dans votre mémoire qu'un des moyens de détecter les infractions aux droits d'auteur est d'insérer des informations utiles ou factices dans le programme

[Text]

did not spring in there spontaneously, it was clearly copied. But assume there was only the essential information in order to conduct word processing, what is in there that is as such creative and is copyrightable? You could not copyright the way in which to shift a manual five-speed transmission.

Assuming that I wanted a word processing program for my computer, presumably I would come up with something similar to the one that you had already developed. How do you establish that you have something that is copyrightable in the first place, that is creative in itself, not just simply empirical information; namely what you need to tell the computer to do to engage in word processing? I do not know if I am making myself clear, the point I am getting at. But it seems to me that there are some functions that are fulfilled by a computer, functions the hardware requires be fulfilled in a particular way, how can you copyright that particular procedure?

Mr. Palmer: This problem is not new with computer software. It has been around ever since copyright has been around. For example, one of the cases from the United States that I am aware of involved whether there would be copyright in a particular form of legal forms that people were manufacturing. It was decided that the legal forms called for certain information and it was not copyrightable to have the forms set up in a certain way because that seemed to be a natural way to set it up; everyone would just automatically do this. I think situations like that would have to be decided on a case-by-case basis, as they are now with books. If people write books on how to drive a car, for example, we think of it as something natural and yet the phrasing is very different.

I am certain that the phrasing is very different between Easy Writer, Word Star, Apple Writer, and all these other types of word processing software packages as well. So I would not be surprised if the expression of those ideas is quite different in the different word processing packages. If it were very, very similar, I certainly would be suspicious.

• 1635

Mr. Beatty: Could I ask you about another area? What about computer-generated art and computer-generated music? That may be a bit of a misnomer, because there is clearly a human component there, but assuming that I bought for my computer a program that would enable me to have so-called computer-generated art or computer-generated music and I liked the product I came up with, who, potentially, would own the copyright? Would I, would the machine, or would the developer of the machine or the software? What you have is an interplay between the machinery itself, the hardware; the software, the programming instructions that are given to it; the operator—and somewhere out of that you get something that is presumably creative and original. What is copyrightable?

Mr. Palmer: I would presume that the art would be copyrightable. Again, I am not a lawyer; I am speaking from

[Translation]

et si on les retrouve dans un autre, cela signifie qu'il a été copié. Mais supposons que votre programme ne contienne que les données essentielles pour le traitement de texte, qu'y a-t-il de si créateur là-dedans pour constituer une propriété intellectuelle? Vous ne pouvez pas réclamer un droit d'auteur sur la façon de changer les vitesses sur une boîte de transmission manuelle.

Si je veux me constituer un programme de traitement de texte pour mon ordinateur, je vais en toute probabilité aboutir à quelque chose de très similaire à ce que vous aurez déjà fait. Comment peut-on déterminer que vous avez créé quelque chose qui puisse être protégé par un droit d'auteur, quelque chose de créateur en soi et qui ne se résume pas à une information simplement empirique, c'est-à-dire les opérations que doit effectuer un ordinateur pour faire du traitement de texte? Je ne sais pas si je m'exprime clairement, mais il me semble qu'un ordinateur remplit des fonctions et dans la mesure où ces fonctions sont dictées par le matériel, comment pouvez-vous revendiquer la propriété de cette procédure?

M. Palmer: Le problème n'est pas seulement apparu avec l'informatique, il s'est toujours posé depuis que les droits d'auteur existent. Par exemple une affaire a été jugée aux États-Unis qui mettait en jeu un droit d'auteur sur un formulaire juridique qu'un éditeur publiait. Il a été décidé que les formulaires juridiques avaient pour objet d'établir certains renseignements et qu'ils ne pouvaient faire l'objet d'un droit d'auteur car tout le monde, naturellement, procéderait de la même façon. Je pense qu'il faudrait trancher cas par cas dans les situations de ce genre comme on l'a fait d'ailleurs avec les livres. Si j'écris un livre sur la façon de conduire une voiture, par exemple, conduire une voiture semble quelque chose de très naturel, mais le texte des différents livres va nécessairement différer.

Je suis sûr que le texte est très différent dans les programmes *Easy Writer*, *Word Star*, *Apple Writer* et tous ces autres types de programme de traitement de texte. Je ne serais pas surpris que ces idées soient exprimées de façon très différente dans ces divers programmes de traitement de texte. S'ils étaient très très proches, j'aurais des soupçons.

M. Beatty: Pourrais-je aborder un autre domaine? Qu'en est-il de la musique ou des oeuvres artistiques produites par ordinateur? Ce n'est peut-être pas entièrement produit par ordinateur, car il doit certainement y avoir une intervention humaine, mais supposons que j'achète pour mon ordinateur un programme qui me permette de produire des oeuvres d'art ou de la musique, qui détiendrait le droit d'auteur de cette oeuvre? Serait-ce moi, serait-ce la machine, serait-ce le concepteur de la machine ou du logiciel? Ce que vous avez là en fait est une interaction entre la machine, c'est-à-dire le matériel, le logiciel, c'est-à-dire les instructions de programmation qu'on lui donne, et l'opérateur: de tout cela sort quelque chose de censément créatif et original. Qu'est-ce qui fait l'objet du droit d'auteur?

M. Palmer: J'imagine que l'oeuvre produite serait protégée par le droit d'auteur. Encore une fois, et je ne suis pas juriste

[Texte]

the point of view of the economic expertise that I bring to this issue. But in a situation like word processing—I do not have a word processor; Professor Flaherty does—what he writes using the word processing package is copyrightable by him, not by the manufacturer of the word processor, not by the developer of the software package that goes with it. I would presume that if he were to do art rather than the verbal analysis that he does he would also be the creator there and would similarly, reasoning by analogy, be entitled to receive the copyright on that art.

Mr. Beatty: Could we move to systems design, chip design in particular? Is that patentable or copyrightable?

Mr. Palmer: That is a tough question. The reason I say it is a tough question is that I am not sure exactly what you mean by chip design.

But let me again argue by analogy to phonograph records. Whoever developed the different types of systems—I am not sure; maybe the various types of systems that competed with each other around the turn of the century . . . There were loads of different systems; there were cylinders and different types of discs that were developed. All of those were patentable in terms of the technology, the systems themselves; but once some music was placed on the record, that particular record and that particular music on the record were not patentable. It might have been copyrightable, but it was not patentable.

We have the same problem, I think, with chips. If by chip design you mean inventing the method of using integrated circuits to plug into a board, that is patentable, I presume.

Mr. Beatty: I have no difficulty with that at all, but assuming that you design a chip, that essentially what you are dealing with is hardware, which is immutable in some way, which inevitably results in being fed certain information results in a specific result, to what extent is it patentable as opposed to copyrightable?

Mr. Palmer: It seems to me it should be copyrightable. The economically efficient thing to do is to have it be copyrightable because the people are producing some creative effort . . . It is imbedded in hard copy, but so are books imbedded in hard copy; it is a set of instructions, but so are many books sets of instructions.

Mr. Beatty: I suppose the idea is really the element here rather than the equipment itself.

Mr. Palmer: Yes. It is the same, I guess, as my answer to the chairman, Mr. Robinson.

Mr. Beatty: Thank you. You have been very helpful. I think I am feeling more confused than when I started, but . . .

Mr. Palmer: I did not intend to confuse you. Ask some more questions. I do not want to leave you confused. Please.

[Traduction]

et je ne peux que parler du point de vue économique. Mais dans le cas du traitement de texte, je n'ai pas de machine de traitement moi-même, mais le professeur Flaherty en a une, tout ce qu'il écrit au moyen de sa machine lui appartient et non pas au fabricant de la machine ni au concepteur du logiciel qui va avec. S'il s'en servait pour produire un dessin plutôt qu'une analyse verbale, il serait également le créateur et jouirait, par analogie, du droit d'auteur sur sa création.

M. Beatty: Pourrions-nous maintenant passer à la conception du système, et notamment à la conception des puces? Est-ce qu'une puce peut faire l'objet d'un brevet ou d'un droit d'auteur?

M. Palmer: C'est une question difficile, d'autant plus que je ne sais pas exactement ce que vous entendez par conception de la puce.

Prenons encore une fois l'analogie des disques de phonographe. Quiconque a mis au point les différents types à l'origine et qui se concurrençaient au début du siècle . . . Il y en avait de toutes sortes, certains étaient des cylindres et il y avait également différents types de disques. Tous ces systèmes pouvaient être brevetés, le brevet portant sur la technologie utilisée, par contre, une fois que de la musique était enregistrée sur le disque, ce disque en particulier et cette musique en particulier ne peuvent plus faire l'objet d'un brevet. Ils sont protégés par le droit d'auteur mais non pas par un brevet.

Je pense que le même problème se pose dans le cas des puces. Si par conception de la puce vous entendez la méthode d'utilisation de circuits intégrés pour former un ensemble, cela peut faire l'objet d'un brevet, je présume.

M. Beatty: D'accord là-dessus, mais supposons que vous conceviez une puce, vous êtes confronté là uniquement à du matériel, qui est d'une certaine façon immuable et qui inévitablement, si on l'alimente avec certaines données, produit les mêmes résultats. Dans quelle mesure cela donne-t-il lieu à un brevet plutôt qu'à un droit d'auteur?

M. Palmer: Il me semble que c'est le droit d'auteur qui devrait s'imposer ici. Ce serait économiquement plus efficace car ceux qui produisent la puce font un effort créateur . . . Cet effort se matérialise par quelque chose de tangible, mais c'est la même chose des livres qui sont imprimés sur papier; la puce donne un ensemble d'instructions, mais c'est également le cas de nombreux livres qui ne sont rien d'autre qu'un ensemble d'instructions.

M. Beatty: C'est plutôt l'idée ici qui compte donc, plutôt que l'équipement lui-même.

M. Palmer: Oui. C'est la même réponse que celle que j'ai déjà donnée au président, M. Robinson.

M. Beatty: Je vous remercie. Vous nous avez été très utile même si j'ai l'impression de m'y retrouver encore moins qu'au début mais . . .

M. Palmer: Je n'avais pas l'intention de semer la confusion. Je vous en prie, posez d'autres questions, je ne veux pas vous laisser dans cet état.

[Text]

Mr. Beatty: Not at all. It is certainly not because of a lack of clarity on your part; it is because of the complexity of the area we are dealing with. It is a constructive confusion, I think, I suffer from. Thank you very much.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I might have one further question for you. You talk about the costs of prosecutions. I am not just sure what context you are talking about there. Were you thinking in terms of the cost to try to get evidence in order to prosecute or for prosecutions; that is, in order to determine detection, how difficult it would be and how costly it would be to detect?

Mr. Palmer: Yes. It seemed to me that there might be some what we call economies of scale in the detection of people who are copying and so on.

• 1640

I know there are computer clubs in every town, in which people get together and exchange software. Well, it does not really pay the developers of the software to sue these clubs, because they are judgement-proof in the first place; they are mostly kids who do not have any assets. If they are not kids, there are not large damages anyway that could be obtained under current copyright provisions. To have to hire spies to go into these computer clubs to detect them and then sue them for damages might be very, very costly, and not worth the effort on the part of the developers of software; whereas there might be some economies of scale that could be taken advantage of by using public enforcement rather than private enforcement of the act.

That is, I think, the major argument that could be made in favour of some form of Criminal Code provisions in this area. But again, I encourage you to think very seriously about why computer software and no other form of intellectual property should be put into the Criminal Code. I do not see a distinction there.

Mr. Beatty: Data in data banks, the raw information itself, is not copyrightable, any more than you could claim copyright on facts included in a book, as such.

Mr. Palmer: I am not sure that is true. I think compilations certainly are copyrightable. They are explicitly included in the Copyright Act. So data would be copyrightable.

Mr. Beatty: Presumably that is data that has been manipulated in a particular way.

Mr. Palmer: Data that I have collected, or data that I have arranged in my own way for a particular compilation that I have selected out of the public domain in some way—people could say it is from the public domain.

Mr. Beatty: But the number of television sets in Canada is not copyrightable in some way.

Mr. Palmer: Right. That is correct.

Mr. Beatty: Or the number of Canadians with an income over \$10,000; or whatever.

[Translation]

M. Beatty: Pas du tout. Ce n'est pas du tout à cause d'un manque de clarté chez vous, c'est dû à la complexité de toute cette question. Je crois que c'est d'une confusion constructive dont je souffre. Je vous remercie infiniment.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'aurais une autre question. Vous parlez du coût des poursuites. Je ne vois pas très bien dans quel contexte vous vous placez ici. Parlez-vous du coût de l'enquête nécessaire pour réunir les preuves en vue des poursuites? Quel serait le coût ou la difficulté de la détection?

M. Palmer: Oui. Il me semble que l'on pourrait réaliser ce que nous appelons des économies d'échelle dans la détection des fraudeurs etc.

Je sais qu'il existe des clubs d'informatique dans chaque ville où les gens se retrouvent pour échanger du logiciel. Les producteurs de ce logiciel n'ont pas grand intérêt à les poursuivre car il s'agit principalement de jeunes qui ne possèdent rien de toute façon. S'il ne s'agit pas de jeunes, la loi actuelle permet déjà de réclamer des dommages-intérêts considérables. Par contre, il pourrait être très coûteux de recruter des espions qui vont s'infiltrer dans ces clubs informatiques pour tenter ensuite des poursuites et cela n'en vaut pas vraiment la peine; par contre, on pourrait réaliser des économies d'échelle si les enquêtes étaient réalisées par des organismes publics plutôt que par des personnes privées.

C'est le principal argument en faveur de l'insertion de dispositions à ce sujet dans le Code criminel. Mais, encore une fois, je vous exhorte à vous demander très sérieusement pourquoi il faudrait inscrire dans le Code criminel le logiciel informatique et en exclure toutes les autres formes de propriété intellectuelle. Je vois mal la distinction entre les deux.

M. Beatty: Les données contenues dans les banques de données, c'est-à-dire les informations brutes, ne font pas l'objet d'un droit d'auteur, pas plus que les faits qui sont publiés dans un livre.

M. Palmer: Je ne suis pas certain que ce soit vrai. Je pense que les compilations de données sont assorties d'un droit d'auteur. Elles sont explicitement mentionnées dans la Loi sur le droit d'auteur. Les données sont donc protégées.

M. Beatty: Mais ne s'agit-il pas là de données qui ont été traitées d'une façon donnée?

M. Palmer: Les données que j'ai recueillies ou que j'ai arrangées à ma façon dans une compilation et que j'ai tiré du domaine public—on pourrait effectivement faire valoir qu'elles appartiennent au domaine public.

M. Beatty: Par exemple, le nombre de téléviseurs au Canada n'est pas une donnée protégée par droit d'auteur.

M. Palmer: Oui, c'est exact.

M. Beatty: Ni le nombre des Canadiens disposant d'un revenu supérieur à \$10,000 ou toute autre statistique de ce genre.

[Texte]

Part of the problem we are trying to deal with in the bill that is before us is the potential damage that could be done to individuals or to institutions as a result of theft of information held in computers which is of some value—it has some utility in itself for the performance of functions by whomever the owner of the data is, presumably. If it is altered or copied or potentially erased, the damage which could be done to the institution that owned the information that inserted it into the data base—that would appear to go well beyond the issue of copyright as such. Have you given any thought to what sort of protection should be accorded to that sort of data contained in a computer?

Mr. Palmer: I have concentrated all my efforts on economic analysis of copyright. I am sure that my esteemed colleague has thought much more seriously about that.

Mr. Beatty: Okay, thank you very much.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I have just one further question, if I may. You have indicated that copyright legislation should be revised clearly to encompass software and firmware products. I wonder if you have any recommendations on the kind of wording that might be used in such a piece of legislation, and if so, would you advise us of same, and if not at this time, and you consider this, would you send it to us?

Mr. Palmer: I have a recommendation: I can only ask that you get a copy of this volume from Consumer and Corporate Affairs. I have been trying to get extra copies myself, so you may have to wait.

There is a chapter in this monograph that talks about the definition of computer software. It defines it pretty much as it has been defined here, as a set of instructions. So I can imagine that in the Copyright Act, in the early part, where it lists all the things that are copyrightable, it could say that computer software would be one of the things; then down later, where it gives definitions, it could say something such as computer software is a set of instructions, etc. I think that would be sufficient for computer software.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So you probably have some words to define the terminology that would be used. They might be helpful to us in preparing a piece of legislation.

Mr. Palmer: I should think the definition of computer software you have here—if you were to talk about putting computer software in the Criminal Code, this definition could be used, yes.

I am sorry; I did not understand that was your question.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you very much for appearing before us, Professor Palmer. If you have any further pearls of wisdom to pass our way, I hope you will feel free to do so before we have to write our report, which is by the middle of next month.

[Traduction]

L'un des problèmes que nous essayons de résoudre au moyen de ce projet de loi, a trait aux préjudices qui peuvent être causés à des personnes ou à des institutions par suite du vol de données entreposées dans un ordinateur et qui représentent une certaine valeur, une utilité propre aux fins de l'exécution de certaines fonctions. Si ces données sont copiées, modifiées ou effacées, le préjudice subi peut dépasser de très loin le champ des droits d'auteur en tant que tel. Avez-vous réfléchi à la protection qu'il faudrait accorder à cette sorte de données mises en mémoire dans un ordinateur?

M. Palmer: J'ai concentré tous mes efforts sur l'analyse économique du droit d'auteur. Je suis sûr que mon distingué collègue y a réfléchi de beaucoup plus près.

M. Beatty: Bien, je vous remercie.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'ai encore une autre question, si vous permettez. Vous avez dit que la Loi sur le droit d'auteur devrait mentionner expressément les logiciels informatiques de toutes sortes. Auriez-vous à nous proposer un texte que nous pourrions insérer dans la loi et peut-être nous le faire parvenir ultérieurement si vous ne l'avez pas ici?

M. Palmer: J'ai une recommandation: je ne peux que vous recommander de demander un exemplaire au ministère de la Consommation et des Corporations. Il vous faudra peut-être attendre car j'ai moi-même du mal à m'en procurer.

Cette monographie contient un chapitre sur la définition du logiciel informatique. On le définit à peu près de la même façon qu'on l'a défini ici, comme un ensemble d'instructions. Je pense donc que la Loi sur le droit d'auteur, dans sa première partie qui dresse la liste de toutes les choses protégeables, pourrait mentionner le logiciel informatique; plus loin, dans le chapitre des définitions, on pourrait dire que le logiciel informatique est un ensemble d'instructions etc. Il me semble que cela suffirait.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez donc probablement un libellé que nous pourrions utiliser. Ce serait utile pour nous de l'avoir.

M. Palmer: Je pense que la définition du logiciel informatique que vous avez ici—si vous deviez parler de logiciel informatique dans le Code criminel, vous pourriez utiliser cette définition, certainement.

Je vous demande pardon, je n'avais pas compris votre question.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je vous remercie d'être venu à notre Comité, professeur Palmer. Si vous avez d'autres idées à nous communiquer, j'espère que vous n'hésitez pas à le faire avant la rédaction de notre rapport qui doit intervenir dans les six semaines.

[Text]

Now I would like to call on Professor David Flaherty, from the University of Western Ontario, to give his words of wisdom to the committee.

• 1645

Mr. David Flaherty (Professor of History and Law, Western University): Mr. Chairman, I have given the clerk of the committee a copy basically of my testimony, and if you have no objection, if that could simply be read into the record, I could then either make a summary statement or even skip the summary statement and simply answer questions, given the kinds of time constraints that either we are living under or you are living under.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Unfortunately, we have not had this statement of yours for a sufficiently long enough period of time for us really to read it and understand it and sort of internalize it as much as we would like to; therefore, although we can append it to the proceedings of today, I think if you would give a sort of overview at this time of your paper, it would be more than helpful to us. Then we will have time for a few questions. We do have a vote in the House of Commons called for, I guess, 5.45 p.m., so we have an hour in which to deal with the matter.

Mr. Flaherty: Thank you, Mr. Chairman.

Basically, despite the rather short notice of your invitation, which I much appreciate—not the short notice but the invitation—I have had an opportunity to do some thinking about an aspect of computer-based crime that, on reading your record, I think you have not heard testimony on before. I mean that a great deal of computer-based crime, or at least some computer-based crime, is going to affect personal information. Personal information is going to be stolen. And basically, while I recognize that most of us think about computer-based crime in terms of stealing somebody's computer or the information that is in a computer or their software or something like that, there are other implications to computer crime that you might as well think about while you are doing this serious study of the computer-based crime area.

I come to this consideration in my background as a privacy advocate, where I will admit that I have usually thought about the protection of privacy in the context of privacy acts and data protection bills. But I note on reviewing the literature in the last few days that generally the literature on computer crime in the United States pays, say, 25% of its attention to privacy and security aspects of the subject. And those are the ones I wish to draw to your attention today.

There are three particular aspects to the privacy implications of computer-related crime. First of all is the risk of unauthorized access to personal information. I would emphasize that I am talking about personal information here as opposed to what is probably the vast bulk of information in

[Translation]

Je donne maintenant la parole au professeur David Flaherty, de l'Université Western Ontario qui va nous éclairer de sa sagesse.

M. David Flaherty (professeur d'histoire et de droit, Université Western Ontario): Monsieur le président, j'ai remis au greffier du comité une copie de mon témoignage essentiel, et si vous n'y voyez pas d'objection, on peut le considérer simplement comme étant lu, aux fins du compte rendu, et je pourrai à ce moment-là soit faire un court résumé ou même laisser tomber le résumé et ne répondre qu'aux questions, étant donné les contraintes de temps qui vous sont imposées et nous sont imposées.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Malheureusement, nous n'avons pas reçu cette déclaration suffisamment à l'avance pour nous permettre de la lire, de la comprendre, de la faire nôtre en quelque sorte, autant que nous l'aurions voulu. Par conséquent, même si nous pouvons l'annexer au compte rendu d'aujourd'hui, cela nous aiderait certainement si vous pouviez nous donner une idée générale de ce qu'elle contient. Nous aurons ensuite le temps de poser quelques questions. Nous devons nous rendre à la Chambre des communes pour un vote à 17h45, je crois, par conséquent nous avons encore une heure pour traiter de la question.

M. Flaherty: Merci; monsieur le président.

De façon générale, en dépit du court préavis de votre invitation, que j'apprécie beaucoup—non pas le court préavis mais l'invitation—j'ai eu l'occasion de réfléchir à un aspect du crime dans le domaine des ordinateurs, et en lisant vos dossiers, je me suis rendu compte que vous n'aviez pas entendu de témoignage à ce sujet jusqu'à maintenant. Je veux dire par là que beaucoup de crimes dans ce domaine, du moins certains crimes reliés aux ordinateurs, auront un effet sur l'information personnelle. On pourra voler cette information. Fondamentalement, je sais que la plupart d'entre nous pensent qu'il s'agit de voler l'ordinateur de quelqu'un ou les renseignements que contient l'ordinateur ou leur logiciel ou quelque chose du genre, mais il y a d'autres répercussions auxquelles il faudrait également songer pendant cette étude très sérieuse des crimes reliés aux ordinateurs.

J'ai décidé d'aborder ce domaine à cause de mes antécédents comme avocat, mais j'admets qu'habituellement je songe plutôt à protéger le droit à la vie privée dans le contexte des lois s'y rapportant et des projets de loi concernant la protection des données. En revoyant ce qui s'est publié au cours des derniers jours, je remarque que de façon générale les crimes reliés aux ordinateurs aux États-Unis portent attention dans 25 p. 100 aux aspects de ce sujet touchant à la protection de la vie privée et à la sécurité. Ce sont ces aspects que je voudrais porter à votre attention aujourd'hui.

Il y a trois aspects aux effets que peut avoir sur la vie privée le crime relié aux ordinateurs. Tout d'abord, le risque de l'accès non autorisé à l'information personnelle. Je soulignerais que je songe ici à l'information personnelle plutôt qu'à l'énorme quantité de renseignements de caractère non

[Texte]

computers, which is non-personal in character. There is the risk of unauthorized access to that information.

Second: once access occurs, there is the risk of unauthorized disclosure of this personal information, with consequences for the individual. And third, it seems to me that the criminal law could wisely direct itself to the need for establishing standards for security in protecting the confidentiality of personal information in computer systems.

I have been surprised recently in conducting a survey with my colleague, Neil Vidmar in London, Ontario, which I think is the first serious study-surveyed data on privacy and public concern for privacy in this country, to discover a very high level of concern for personal privacy among the 200 households that we surveyed in the context of a survey on peoples' attitudes toward new technology. As the Canadian public thinks about microtechnology and the new infomatics and all the rest of it, their most important social concern is for the protection of their privacy. That is one of the reasons why I think that in the context of computer-based crime, it would be very desirable to have some indirect protections for personal privacy added in.

This judgment also is reinforced by my own view that except for the Province of Quebec, provincial protections for personal privacy are non-existent in terms of protecting personal information, especially in automated form. The private sector in this country is almost totally unregulated when it comes to the collection, storage and dissemination, of personal information. The only exception in the Province of Quebec, and I have discussed that in my prepared statement.

So I am thinking that in terms of your proposed legislation on computer-related crime, you should consider the interests of data subjects as well as the interests of data owners. People constantly ask privacy advocates, Why do you think there are any problems in this area that we should be concerned about?

• 1650

In my written testimony, I have summarized some findings of the very famous Krever commission report on the confidentiality of health records in Ontario, which demonstrates in gory detail the kinds of risks to our personal privacy that exists from automated personal information systems in general and automated health information systems in particular. I would submit to you, Mr. Chairman, that generally speaking, when it comes to the computerization of personal information, the interests of efficiency are rated much more highly than interests in protection of privacy or even in the maintenance of appropriate security standards.

I participated in a security conference in Chicago last week, and the main result I took away from this gathering was an astonishing reinforcement of a view that lay people find astonishing; that is, most large computer systems are very inadequately protected when it comes to security. That is why

[Traduction]

personnel que contient l'ordinateur. Il y a le risque d'un accès non autorisé à ces renseignements.

Deuxièmement, une fois qu'on y a eu accès, il y a le risque d'une divulgation non autorisée de ces renseignements personnels, avec les conséquences que cela suppose pour le particulier. Troisièmement, j'ai l'impression que le droit criminel serait sage d'étudier le besoin d'établir des normes pour la sécurité afin de protéger l'aspect confidentiel des renseignements personnels contenus dans les systèmes informatisés.

J'ai fait une enquête récemment avec mon collègue Neil Vidmar de London, Ontario, c'est je crois la première enquête sérieuse relative aux données sur la vie privée et la préoccupation qu'elle pose pour le public au pays, et j'ai été surpris de découvrir dans les deux cents foyers que nous avons visités dans le contexte de cette enquête sur l'attitude des gens vis-à-vis la nouvelle technologie que beaucoup s'inquiétaient de ce droit à la vie privée. Le public canadien s'intéresse à la microtechnologie et à ce nouveau domaine de l'informatique, et tout le reste, mais dans notre société, on se soucie surtout de protéger son droit à la vie privée. C'est une des raisons pour lesquelles, dans ce contexte du crime relié aux ordinateurs, il serait souhaitable pour protéger le droit à la vie privée des personnes d'y incorporer un système indirect ou de protection.

Outre cela, je pense également que sauf pour la province de Québec, les protections provinciales du droit à la vie privée pour les personnes n'existent pas, dans ce sens qu'on ne protège pas l'information personnelle, si elle est informatisée. Le secteur privé au pays est peu ou pas réglementé lorsqu'il s'agit de faire la collecte, d'entreposer et de distribuer l'information personnelle. La seule province qui fait exception, c'est le Québec, et j'en ai parlé la déclaration que j'ai préparée.

Je crois donc qu'une loi concernant le crime relié aux ordinateurs devrait tenir compte de l'intérêt des sujets de ces données de même que de l'intérêt des propriétaires de données. Les gens préconisent constamment le droit à la vie privée, pourquoi croyez-vous qu'il nous faudrait nous préoccuper des problèmes dans ce domaine?

Dans mon témoignage écrit, j'ai résumé certaines conclusions du rapport de la très célèbre commission Krever sur l'aspect confidentiel des dossiers relatifs à la santé en Ontario, qui souligne dans tous les détails les plus horribles le genre de risques que représentent pour notre droit à la vie privée les systèmes automatisés relatifs à l'information personnelle et surtout les systèmes automatisés relatifs à l'information sur la santé. Je soutiens, monsieur le président, que de façon générale, lorsqu'il s'agit de l'informatisation de l'information personnelle, on tient davantage compte de l'efficacité que de la protection du droit à la vie privée ou même de la conservation des normes appropriés pour la sécurité.

J'ai assisté à une conférence sur la sécurité à Chicago la semaine dernière, et cette réunion m'a confirmé de façon étonnante une opinion que les profanes trouvent également étonnante, c'est-à-dire que la plupart des grands systèmes d'ordinateurs ne sont pas adéquatement protégés sur le plan

[Text]

I think the criminal law will probably have to step in and mandate some minimum standards for security; otherwise, large systems are not using the appropriate protections that are available to them.

Now, in thinking about privacy and security in connection with computer-based crime, I took the opportunity to review some foreign legislation that touches on the three points on which I think you should consider some criminal legislation; that is, the question of unauthorized disclosure, unauthorized access, and the need for security standards. In my written statement I have reviewed legislation from countries I work in regularly: Sweden, United States, Germany, France, and the United Kingdom. I do not include the Province of Quebec as a foreign country, obviously, but I did put in something about that and the international efforts of OECD and the council of Europe.

I think the subcommittee should be particularly interested in a data protection bill that is before the British House of Commons at the moment, which was already passed by the House of Lords in March. It has particular importance for other English-speaking countries because it adopts a European system of data protection for both the public and private sectors. This is the first data protection bill in an English-speaking country that regulates the private sector; it establishes a series of controls that I discussed in my written statement on unauthorized disclosure, unauthorized access, and the setting of a minimum standards.

Let me just quote one provision. The law says:

Another basic principle of data protection for personal information in the hands of registered data users or computer bureaux is that "appropriate security measures shall be taken against unauthorized access to or alteration, disclosure or destruction of personal data".

There are criminal sanctions built into that legislation for breach of it. I think in the language of some of these foreign laws that I have given to you in my written statement, you will find language that would be appropriate for addressing, in your proposed legislation, some of the issues I have read.

Now, I have just one more example, because it is close to home in one sense. The Organization for Economic Co-operation and Development has guidelines on the protection of privacy and transport of flows of personal data. It is a source of some discomfort to me that Canada is one of only three member nations of OECD that have not yet signed these guidelines.

One of the principles in the guidelines is:

that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

[Translation]

sécurité. C'est la raison pour laquelle le droit criminel devra probablement étudier la chose et exiger que des normes minimales soient imposées, car les systèmes importants ne se servent pas des protections appropriées qui sont à leur disposition.

J'ai réfléchi au droit à la vie privée et à la sécurité en rapport avec les crimes reliés aux ordinateurs, et j'ai saisi cette occasion pour revoir certaines lois étrangères qui touchent aux trois questions sur lesquelles il faudrait vous pencher, à mon avis, pour l'étude d'une loi criminelle. Il s'agit de la question de la divulgation non autorisée, de l'accès non autorisé et du besoin de normes de sécurité. Dans ma déclaration écrite, j'ai examiné les lois qui existent présentement dans des pays où j'ai travaillé de façon régulière, la Suède, les États-Unis, l'Allemagne, la France et le Royaume-Uni. Je n'inclus pas la province du Québec comme pays étranger, évidemment, mais j'ai mentionné quelque chose à son sujet de même que les efforts internationaux que font l'OCDE et le conseil de l'Europe dans ce domaine.

A mon avis, le Sous-comité devrait particulièrement s'intéresser à un projet de loi concernant la protection des données dont fait présentement l'étude la Chambre des communes britannique, il a déjà été adopté en mars par la Chambre des Lords. Ce projet de loi est particulièrement important pour d'autres pays de langue anglaise, car il adopte un système de protection de données européen pour les secteurs public et privé. C'est le premier projet de loi sur la protection des données, dans un pays anglophone, qui régleme le secteur privé. Il prévoit une série de contrôles que j'explique dans ma déclaration écrite sur la divulgation non autorisée, l'accès non autorisé et l'établissement de normes minimales.

Permettez-moi de citer une de ces dispositions. La loi déclare:

Un autre principe de base sur la protection des données concernant l'information personnelle entre les mains des utilisateurs de données autorisés ou de bureaux d'ordinateur, c'est que «des mesures de sécurité appropriées doivent être prises contre l'accès ou les changements non autorisés, la divulgation ou la destruction de données personnelles».

Cette loi contient des sanctions criminelles pour toute contravention. Le libellé de ces lois criminelles étrangères que je vous donne dans ma déclaration écrite, vous montrera qu'un libellé serait approprié pour aborder certaines questions, que je vous ai lues, dans votre projet de loi.

Permettez-moi de vous donner un autre exemple, qui s'apparente un peu à notre situation. L'Organisation de coopération et de développement économiques a des directives pour la protection du droit à la vie privée et le transport des masses de données personnelles. Je trouve malheureux que le Canada soit l'un des trois seuls membres de l'OCDE qui n'ait pas signé ces directives.

Un des principes contenus dans ces directives est le suivant:

que les données personnels devraient être protégées par des garanties de sécurité raisonnables contre les risques comme la perte ou l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation de données.

[Texte]

Canada is presumably going to sign these guidelines in the fullness of time. I would expect some of our leading companies to also sign the guidelines. I think it might be useful to further raise the consciousness of provincial governments and the private sector by putting a statement such as that into our criminal law.

I also discuss the fact that Bill 65 in Quebec on access to public documents and the protection of personal information, passed in 1982—which is unfortunately not well enough known in Canada as a whole and which is, in fact, I regret to say, even stronger than our new federal privacy legislation in adopting a strong bureaucracy to implement access to information and the protection of personal privacy—also has some of these kinds of measure that I have been citing to you from foreign legislation.

• 1655

In summary, Mr. Chairman, I suggest to you that if you are considering criminal legislation on computer-related crime, I think it is desirable that you include some sanctions that would have the indirect benefit of protecting the privacy of residents of Canada, or non-residents of Canada, who have information about themselves entered into the numerous data banks and information systems that exist.

Secondly, I think a particularly valuable by-product of such legislation would be to make up for the great lacuna in current legislation at the provincial levels and in the private sector. I think, even if one cannot anticipate any great spate of prosecutions under this kind of legislation, the basic effect of making unauthorized access and unauthorized disclosure of personal information criminal offences would be to alter significantly the consciousness of holders of personal information as to what their responsibilities are for the protection of privacy. I think that would be of considerable benefit to the citizenry as a whole.

Thank you, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): Thank you for your remarks, Professor Flaherty.

Do you wish to commence, Mr. Beatty, or do you want me to...?

Mr. Beatty: Thank you, Mr. Chairman.

Let me first of all thank Professor Flaherty and say that, notwithstanding the short period of time you have had for preparation, you have introduced a number of ideas that have not been considered by the committee before that are both novel and stimulating, in particular the suggestion of mandatory levels of security to be included in the law. By and large, what we have been dealing with in the context of my bill has been the issue of where unauthorized access had taken place and then what actions could be taken.

[Traduction]

Le Canada va probablement signer ces directives en temps et lieu. Je m'attends à ce que certaines de nos compagnies dirigeantes signent également ces directives. Ce serait peut-être utile de le rappeler aux gouvernements provinciaux et au secteur privé et ajoutant une telle déclaration dans notre droit criminel.

Je veux parler également du fait que le projet de loi 65 au Québec concernant l'accès aux documents publics et la protection de l'information personnelle, adopté en 1982, n'est malheureusement pas suffisamment connu dans l'ensemble du Canada et, j'ai le regret de le dire, il est plus puissant que notre nouvelle loi fédérale sur le droit à la vie privée dans ce sens qu'il a recours à une forte bureaucratie pour la mise en vigueur de l'accès à l'information et de la protection du droit à la vie privée, et ce projet de loi contient également ces genres de mesures que j'ai mentionnés en rapport avec les lois étrangères.

Pour résumer, monsieur le président, si vous songez à recourir à des dispositions du droit pénal pour les crimes reliés aux ordinateurs, il serait souhaitable, à mon avis, d'inclure certaines sanctions qui indirectement pourraient protéger le droit à la vie privée des résidents du Canada, ou des non-résidents, pour lesquels certains renseignements personnels sont entrés dans les nombreuses bandes de données et systèmes d'information.

Deuxièmement, comme sous-produit important d'une telle législation, il faudrait combler cette lacune importante que contient la loi actuelle, au niveau des provinces, et également dans le secteur privé. Même si on ne prévoit pas un grand nombre de poursuites dans le cadre de cette loi, elle aurait pour effet surtout de faire de l'accès non autorisé et de la divulgation non autorisée des renseignements personnels des crimes et elle modifierait également de façon importante l'attitude des détenteurs de l'information personnelle quant à leurs responsabilités pour la protection des renseignements personnels. Ce serait extrêmement avantageux pour tous les citoyens.

Merci, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je vous remercie pour ces remarques, professeur Flaherty.

Voulez-vous commencer, monsieur Beatty, ou voulez-vous que je...?

M. Beatty: Merci, monsieur le président.

Permettez-moi tout d'abord de remercier le professeur Flaherty et de souligner qu'en dépit du court préavis qu'il avait reçu, il nous a présenté un certain nombre d'idées qui n'avaient pas été étudiées en Comité auparavant. Elles sont à la fois nouvelles et stimulantes, je songe surtout à la suggestion d'inclure dans la Loi des niveaux de sécurité obligatoires. De façon générale, dans le contexte de mon projet de loi, nous avons traité surtout des endroits où se sont produits des accès non autorisés et des mesures qui pourraient être prises.

[Text]

What other jurisdictions, which you are aware of, have legislation that specifically mandates appropriate levels of security on computerized information? And do they differentiate between computerized information and information held in manual form?

Mr. Flaherty: The usual reason for excluding manual records is simply the enormous scope of manual records in our society and the gradual trend towards putting everything that is possible into an automated system.

I cannot give you, without going through the data in my report, an exact run-down of which countries have minimum security standards, but my recollection is that all the pieces of legislation I have quoted have followed the OECD or council of Europe's convention in recommending that security be included as desirable for any personal information system.

For example, the European convention, which is very significant because it will probably be ratified and come into force this year—it is the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data—says that:

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

A further article of the convention says that parties to the convention, which will include all the European members of the council of Europe, 15 or so, eventually, have to put sanctions and remedies for violations of this provision in their domestic law.

I have quoted the legislative resource manual on computer crime of the U.S. Department of Justice, the Bureau of Justice Statistics, and their third chapter reviews federal and state legislation on minimum security standards.

In fact, now that you have warmed me up, I think I remember that the Privacy Act of 1974 also requires, in subsection (10), the maintenance of appropriate security safeguards:

to insure the security and confidentiality of records
etc., etc.

Mr. Beatty: That is in the public sector as opposed to the private sector?

Mr. Flaherty: Yes, in the public sector as opposed to the private sector. And the state laws... there are about 10, 15, or 20 state laws on computer-related crime; they also are primarily public sector. But as you are well aware, Mr. Beatty, there is enormous resistance to legislating for the private sector in North America generally, which is why I think the initiative of Margaret Thatcher's government is so interesting; she is legislating with a very heavy hand for the private sector,

[Translation]

Quelles sont les autres compétences que vous connaissez, qui disposent de lois prévoyant des niveaux de sécurité obligatoire pour les renseignements informatisés? Est-ce qu'on fait la différence entre l'information informatisée et l'information conservée «manuellement»?

M. Flaherty: La raison habituelle qu'on invoque pour exclure les dossiers manuels, c'est simplement qu'ils constituent une masse énorme dans notre société et qu'on a tendance de plus en plus à enregistrer tout ce qui est possible d'enregistrer dans un système automatisé.

Je ne puis pas vous donner, sans reprendre toutes les données que contient mon rapport, une liste exacte des pays qui ont adopté des normes de sécurité minimales, mais si je me souviens bien, tous les textes législatifs que j'ai cités ont suivi des directives de l'OCDE ou la convention du Conseil de l'Europe pour recommander que la sécurité soit incluse comme élément souhaitable à tout système sur l'information personnelle.

Ainsi, la Convention européenne, qui est très importante car elle sera probablement ratifiée, et entrera en vigueur cette année—il s'agit de la convention du Conseil de l'Europe pour la protection des particuliers en ce qui a trait au traitement automatique des données personnelles—cette convention déclare...

Des mesures de sécurité appropriées doivent être prises pour protéger les données personnelles conservées dans les dossiers de données automatisées contre tout accident ou destruction non autorisée ou perte accidentelle et également contre l'accès non autorisé, le changement ou la distribution.

Un autre article de la convention stipule que les parties à la convention, qui comprend tous les membres européens du Conseil de l'Europe, 15 environ, devront éventuellement prévoir des sanctions et des solutions pour toutes contraventions à cette disposition de leur loi interne.

J'ai cité le manuel de ressources législatif sur le crime relié aux ordinateurs du ministère de la Justice des États-Unis, le Bureau des statistiques juridiques, et leur troisième chapitre examine les lois fédérales et les lois des États en ce qui a trait à des normes de sécurité minimales.

Maintenant que vous m'avez un peu stimulé, je crois me rappeler que la Loi sur la protection de la vie privée de 1974 exige également, au paragraphe 10, le maintien de garanties appropriées pour la sécurité:

pour garantir la sécurité et l'aspect confidentiel des dossiers.
... etc., etc.

M. Beatty: C'est pour le secteur public par opposition au secteur privé?

M. Flaherty: Oui, c'est pour le secteur public par opposition au secteur privé. Dans les lois des États... Il y a je crois 10, 15 ou 20 lois des États sur les crimes reliés aux ordinateurs, elles touchent surtout au secteur public. Comme vous le savez, monsieur Beatty, le secteur privé en Amérique du Nord oppose énormément de résistance à une telle législation, c'est pourquoi l'initiative du gouvernement de Margaret Thatcher est si intéressante. Elle légifère d'une main très ferme pour le secteur

[Texte]

requiring that every user of automated personal information in Great Britain register with the Data Protection Registrar.

Mr. Beatty: Could you discuss for me the potential here? I guess one example of a data base that is rapidly going on line is for a banking system where I can access my account remotely by going into any branch of Canada Trust, in my case, virtually anywhere in the country. What you are proposing would be minimum security standards and that sanctions could be taken against a bank, or a trust company, that had its system violated in some way if they had not met those standards?

• 1700

Mr. Flaherty: I think banking is a very good area to discuss. I did some work for the Ministry of the Attorney General in Ontario in 1977 as part of a task force in electronic funds transfers; my area was privacy, confidentiality, and security. And I am absolutely astonished—perhaps I should not be, or perhaps it is a reflection that I am an academic—that the 1980 revision, or 1981 revision of federal Bank Act still does not contain any statutory requirements for protecting the confidentiality of personal information in our banking system in this country.

Now, the banks will tell you they have policies on confidentiality and security and privacy. In fact, the Bank of Montreal was wise enough last year to codify these into a lovely blue pamphlet. But the fact of the matter is there is no statutory protection for the confidentiality of my information or your information in our banking system. And I would also admit, six years after I did that research, that I was guilty of a typical failure. That is, I talked to lots of vice-presidents, including one at Canada Trust, who told me that their policy was absolute confidentiality on customer information. Unfortunately, I have also talked to lots of people who work for banks and the realities are much different. There is still personal information being given out over bank counters by bank managers and bank tellers to all kinds of people who should not be getting it, or who have not established a legitimate right to obtain data in that fashion. And I am thinking about law enforcers in particular.

We have nothing remotely comparable in this country to the Right to Financial Privacy Act in the United States of 1978, which was at least to establish minimum due process standards before law enforcements agencies could obtain access to my bank account or yours.

I think the banks, because of the financial value of the information they hold, have substantially improved their security systems in recent years. However, I still feel we would be better off, in every piece of legislation possible, spreading

[Traduction]

privé, en exigeant que chaque utilisateur d'information personnelle automatisé en Grande-Bretagne s'inscrive auprès du registraire de la protection des données.

M. Beatty: Pouvez-vous nous dire ce que cela représente ici? Un des exemples de base de données auxquelles on a facilement accès, c'est celui du système bancaire, où je puis avoir accès à mon compte à partir de n'importe quelle succursale du *Canada Trust*, dans mon cas, n'importe où au pays. Vous proposez des normes de sécurité minimales et des sanctions qui pourraient être prises contre une banque, ou une fiducie, si son système était enfreint de quelque façon pour ne pas avoir respecté ces normes?

M. Flaherty: Je crois que le système bancaire peut fournir une discussion intéressante. J'ai fait un certain travail pour le Procureur général de l'Ontario en 1977, en participant au groupe de travail sur les transferts électroniques de fonds. Je m'occupais personnellement de la protection des renseignements personnels, de l'aspect confidentiel et de la sécurité. Je suis tout à fait étonné—je ne devrais peut-être pas l'être, cela résulte peut-être du fait que je suis un universitaire—que la révision de 1980 ou celle de 1981 de la Loi sur les banques du gouvernement fédéral ne contenait aucune exigence statutaire pour protéger l'aspect confidentiel des renseignements personnels dans le système bancaire du pays.

Les banques vous diront qu'elles ont des politiques concernant l'aspect confidentiel et la sécurité de même que les renseignements personnels. En réalité, la Banque de Montréal a sagement décidé de codifier l'an dernier ces questions dans un très joli dépliant bleu. Il n'en demeure pas moins qu'il n'y a aucune protection statutaire pour l'aspect confidentiel de mes renseignements ou des vôtres dans notre système bancaire. J'admets également, six ans pour avoir fait cette recherche, que j'ai été coupable d'un échec typique. Autrement dit, j'ai discuté avec un grand nombre de vice-présidents, y compris celui de Canada Trust, qui m'ont dit que leurs politiques visaient à un aspect confidentiel absolu pour tout renseignement concernant le client. Malheureusement, j'ai également parlé à beaucoup de gens qui travaillent dans les banques et la réalité est bien différente. Les gérants de banques et les caissiers donnent toujours des renseignements personnels, au comptoir, à toutes sortes de gens qui ne devraient pas les obtenir, ou qui n'ont pas établi leurs droits légitimes à obtenir des données de cette façon. Je pense par exemple à ceux qui sont chargés d'appliquer la loi.

Nous n'avons rien de comparable au pays au droit à la Loi sur la protection des renseignements financiers *Right to Financial Privacy Act* qu'ont adoptée les États-Unis en 1978, qui visait à établir au moins des normes minimales par procédures judiciaires avant que les préposés à l'application de la loi puissent avoir accès à mon compte de banque ou au vôtre.

A cause de la valeur financière des renseignements qu'elles détiennent, je crois que les banques ont beaucoup perfectionné leurs systèmes de sécurité ces dernières années. Cependant, je crois toujours que nous serions mieux protégés, par un texte de

[Text]

the principles of data protection. That is, the Bank Act should say that a person's bank information should be confidential except under circumstances 1, 2, and 3. There may be legitimate reasons where you would not want to keep it confidential, but I would like to see that established by statute.

That is one of the reasons why, since data protection has not spread in this country the way it has in West Germany or Sweden, where every piece of legislation that involves personal information, whether it is police, national security, social welfare, labour, anything, census . . . In West Germany they put in a data protection provision saying there are rules against unauthorized access to the data, unauthorized disclosure of it, and usually some type of review mechanism that requires the custodians of the information to have appropriate security measures to keep it confidential.

Mr. Beatty: Assume that my bank or trust company had developed data protection standards they felt were satisfactory to protect their system, and they end up having their data base violated; my information is taken. Their data protection standards have not met standards which you felt would be acceptable, although they felt it was good enough at the time, should my remedy be a civil remedy or should we be using the Criminal Code?

Mr. Flaherty: You see, right now, under typical concerns for computer-based crime, we would be interested in helping the outraged Bank of Nova Scotia to remedy this gross abuse to its information system. I think that is quite desirable; I think that it is unfortunate we do not yet have criminal sanctions prohibiting that kind of behaviour. On the other hand, I also would remind you I am the individual whose data may have been stolen, and there may also be harms that I have suffered—to my privacy, for example—as a by-product of this theft of information. Someone may have stolen it to use it in a way that would harm me. What are my remedies?

Unlike the United States, and this is perhaps the desirable aspect of Canada, it is very difficult to sue anybody for anything very useful in this country, the kinds of damages you can get for something like invasion of privacy or mental harm, or, say, I felt terrible, I felt embarrassed for three whole weeks because somebody knew my income was only *X* amount per year, you cannot get much for that in this country.

I think there should be criminal sanctions against the individual who is engaged in the criminal act of entering a particular information system and taking out the data—even if they do not do anything with it. There has been a violation of

[Translation]

loi, qui identifierait les principes de la protection des données. Autrement dit, la Loi sur les banques devrait stipuler que les renseignements bancaires concernant une personne devraient être confidentiels sauf dans les cas 1, 2 et 3. On peut avoir des raisons légitimes pour ne pas vouloir conserver cet aspect confidentiel, mais je voudrais que la loi l'établisse.

C'est une des raisons pour lesquelles, étant donné que la protection des données ne se fait pas à l'échelle du pays, comme cela se fait en Allemagne de l'ouest ou en Suède, où chaque texte législatif qui a trait à des renseignements personnels, que ce soit pour les policiers, la sécurité nationale, l'assistance sociale, le travail ou toute autre chose, le recensement . . . En Allemagne de l'ouest, on a adopté une disposition pour la protection des données qui prévoit des règlements contre l'accès non autorisé aux données, la divulgation non autorisée, et habituellement une sorte de mécanisme d'examen qui prévoit pour les «gardiens d'information» des mesures de sécurité appropriées afin qu'ils puissent garder ces données confidentielles.

M. Beatty: En supposant que ma banque ou ma société de fiducie adopte des normes pour la protection des données, satisfaisantes à leur avis pour protéger leur système, et qu'il y ait infraction à leur base de données, mes renseignements sont divulgués. Leurs normes de protection des données ne répondent pas aux normes qui, à votre avis seraient acceptables, même si la banque ou la fiducie croit qu'elles sont suffisamment bonnes, est-ce que je devrais à ce moment-là prendre des mesures au civil ou me servir du Code criminel?

M. Flaherty: Actuellement, à cause des préoccupations que soulèvent les crimes reliés aux ordinateurs, nous serions intéressés, voyez-vous, à aider la Banque de la Nouvelle-Écosse contre laquelle on aurait commis un crime, pour remédier à cet abus évident dans le système d'information. C'est tout à fait souhaitable à mon avis, mais je crois qu'il est dommage que nous n'ayons pas présentement de sanctions criminelles qui empêchent ce genre de comportement. Par ailleurs, je vous rappelle également que je suis la personne à qui on a volé des renseignements, et je peux avoir subi des dommages—à ma vie privée par exemple—suite à ce vol de renseignements. Quelqu'un peut les avoir volés pour s'en servir de façon à me causer du tort. Quels recours ai-je?

Contrairement aux États-Unis, et c'est peut-être un aspect souhaitable ici au Canada, il est très difficile de poursuivre quelqu'un pour quoi que ce soit d'utile au pays, les genres de torts que vous pourriez subir à cause de l'invasion de votre vie privée ou de torts sur le plan mental, ou disons que c'est tout à fait terrible, je me sens embarrassé pendant trois semaines parce que quelqu'un connaît mon revenu, ce que je gagne par année, vous ne pouvez pas vraiment obtenir quoi que ce soit ici au Canada à cause de ce genre de tort.

• 1705

Il devrait y avoir, à mon avis, des sanction criminelles de prises contre toute personne qui commet un acte criminel du fait qu'elle a accès à un système d'information et qu'elle en tire des données . . . même si elle ne fait rien avec ces données. Il y a eu violation de mes droits, en tant qu'abonné ou participant à

[Texte]

my rights as a subscriber or a participant in a banking scheme, a life insurance scheme, or the census for that matter.

Mr. Beatty: One thing about the institutions... What sanctions would you see... You would argue as well that the banks should have charges laid against them if they have not taken appropriate care.

Mr. Flaherty: Yes. I would admit that I have some reluctance to try to make the argument that criminal charges should be brought against a bank or a trust company for failure to maintain adequate security standards. On the other hand, I am finding it very difficult to understand how we are going to persuade banks, loan companies, and every other kind of organization in our society to maintain the proper security standards. Banks, in the case of security, are perhaps not our best example.

Mr. Beatty: Take, for example, universities then. There is the celebrated University of Alberta case where the data base was damaged and where, I believe, employees' personnel records were affected. Unless I am mistaken, obscenities were printed on peoples' pay cheques. I am not sure whether the individuals involved were alleged to have had access to how much money, for example, individuals would be paid. In your judgment, then, should there have been a provision in the law that a university whose data base was violated should have criminal charges laid against it in some way?

Mr. Flaherty: I think we could use personnel records, generally. Someone may simply be fishing in the personnel records of an organization. It could be the House of Commons, or it could be any federal, provincial, or private company. Personnel records today should ideally be cleaned up and should not contain a lot of the garbage they have traditionally contained from a privacy point of view. You do not need a lot of the stuff that people have traditionally collected.

However, if it is an automated form, somebody who is fishing around in the computer files could come up with your entire profile as an employee of company X and know a great deal about you. I know that some of the major companies in this country target young employees for their future. They predict after several years what their target is going to be, how far they are going to go in the company; they monitor them very carefully. I would not be surprised if a lot of that information is automated. Why would a fellow competitor not try to get access to the system to try and find out how his peers are going to do, or find out exactly how they think about him. It would not be exactly an invasion of privacy to access your own data. It would be, more clearly, simply a breach of the company's interests.

As you well know, we have nothing much more that will happen to somebody who does that kind of thing than get fired. You might say that is a pretty heavy sanction, and it certainly is. But I think, based particularly on reading the previous testimony, that you have heard from CBEMA and from the computer security experts, I am struck by the extent

[Traduction]

un système bancaire ou d'assurance-vie, ou même à un recensement.

M. Beatty: Au sujet des institutions... Quelles seront les sanctions... Vous pourriez prétendre également que les banques pourraient être accusées si elles n'ont pas pris les mesures nécessaires.

M. Flaherty: Oui. J'admets que je soulèverais cet argument avec réticence quant aux accusations criminelles qui pourraient être portées contre une banque ou une fiducie qui n'avait prévu aucune norme adéquate de sécurité. Par ailleurs, il m'est très difficile de savoir comment nous pouvons persuader les banques, les compagnies de prêts, et tout autre genre d'organisations dans notre société qu'il faille avoir des normes de sécurité adéquates. Dans le cadre de la sécurité, les banques ne sont peut-être pas notre meilleur exemple.

M. Beatty: Prenons, par exemple, les universités. Il y a le cas très célèbre de l'université de l'Alberta dont la base de données a été endommagée et où, je crois, les dossiers personnels des employés ont été touchés. Si je ne me trompe, des obscénités ont été imprimées sur les chèques de paie des employés. Je ne sais pas si les personnes en cause ont eu accès aux montants des sommes versées aux particuliers. À votre avis, la loi n'aurait-elle pas dû comprendre une disposition pour que l'université, dont la base de données a été violée, puisse être l'objet d'accusations criminelles d'une façon ou d'une autre?

M. Flaherty: Pour répondre de façon générale, je crois qu'on peut se servir des dossiers personnels. Quelqu'un peut simplement chercher à obtenir des renseignements des dossiers personnels d'une organisation. Ce peut être la Chambre des communes, ce peut être le gouvernement fédéral, provincial ou une compagnie privée. Les dossiers personnels devraient idéalement, de nos jours, être nettoyés et ne pas renfermer toutes ces choses inutiles qu'ils ont toujours conservées du point de vue renseignement personnel. On n'a pas besoin d'une grande partie des renseignements que les gens collectent de façon traditionnelle.

Cependant, si les renseignements sont informatisés, quelqu'un qui joue avec des dossiers de l'ordinateur peut obtenir le profil complet d'un employé d'une compagnie et très bien se renseigner à votre sujet. Je sais que certaines grosses compagnies au pays identifient de jeunes employés quant à leur avenir. Ils prédisent après plusieurs années l'objectif qu'ils auront atteint, jusqu'où ils peuvent se rendre dans la compagnie, ils les surveillent de très près. Je ne serais pas surpris qu'en grande partie ces renseignements soient automatisés. Pourquoi un concurrent n'essaierait-il pas d'avoir accès au système pour voir ce que ses pairs vont faire, pour savoir exactement ce qu'on pense de lui. Ce ne serait pas exactement une invasion de la vie privée que d'avoir accès à ses propres données. Ce serait plutôt un manquement aux intérêts de la compagnie.

Vous le savez très bien, rien d'autre ne peut arriver à cette personne que de se faire congédier. Vous pouvez me répondre qu'il s'agit d'une sanction assez sévère, et ce l'est certainement. Après avoir lu les témoignages précédents, vous avez entendu, je crois, la CBEMA et les experts de la sécurité en matière d'ordinateurs. Je suis frappé de voir que vous voulez rendre les

[Text]

to which you are engaged in a consciousness-raising effort here. The ultimate way of raising consciousness in our society about anything is to make it a crime.

One of the other things I do is write about the history of criminal justice in periods of time that would not interest you—the 17th and 18th centuries. I know how the criminal law has been abused over time, and applied to too many things. I know the tendency today is to decriminalization, to restrict the scope of the criminal law. I do not very easily say to you, then, that I think you ought to start extending criminal sanctions to this particular area. But I cannot think of any other way that is going to draw to peoples' attentions the fact that there are certain things you may want to do to computers, and particularly the personal information in those computers, that you simply ought not to do. That it is immoral; it is unethical; it is also criminal. If you do some of these things you are going to run the risk of prosecution.

Going back to universities, people are regularly engaging in fishing expeditions into other peoples' files in university computer systems. We can agree it is immoral; we can agree it is unethical; it is maybe contrary to a written agreement you signed as a user of the computer system. But perhaps the only way to get through to some of these peoples' thick heads that they should not do this kind of thing is to include a provision in the Criminal Code, which I have no doubt would be rarely used. Nevertheless, you would only need a few prosecutions to really wake people up. It is like under the Privacy Act of 1974 in the United States; it has criminal sanctions against unauthorized disclosure of personal information. There have only been a few punishments, successful prosecutions, under that act; but you do not need that many to raise peoples' consciousness.

Mr. Beatty: I think there is a strong consensus. I have no difficulty, and I do not think anybody does particularly, with the argument that sanctions should be able to be taken against the person who violates the data base.

• 1710

I think the novel suggestion that you are making is that the owner of the data base, if he has not followed proper security standards, should be himself liable. The only analogous situation that springs to mind is under firearms legislation, where if I am storing firearms at home and my house is burgled and somebody takes them and I have not properly put them away, charges may be laid against me as well. But if I had a store downtown and somebody broke into my store and stole TV sets I was planning to sell, I would not imagine that charges would be laid against me for not having a proper lock on the door.

What you are proposing is something that is a relatively new departure. I suppose on the grounds of injury to third parties, as one would argue in the case of the gun control legislation

[Translation]

gens plus conscients de ce qui peut arriver dans ce domaine. La façon de le faire surtout, c'est de faire de cette infraction un crime.

Un des autres sujets sur lequel j'ai écrit, c'est l'histoire de la justice criminelle au cours de périodes qui ne vous intéressent pas... les 17^e et 18^e siècles. Je sais comment le droit criminel a fait l'objet d'abus, il visait trop de choses. Je sais qu'on a tendance aujourd'hui à tout décriminaliser, à limiter l'envergure du droit criminel. Ce n'est pas facile pour moi de vous le dire, mais je pense qu'il faudrait commencer par élargir les sanctions criminelles dans ce domaine particulier. Je ne vois pas d'autres façons de le faire que de porter à l'attention des gens le fait qu'on peut vouloir faire certaines choses avec l'ordinateur et, surtout, avec les renseignements personnels que contiennent ces ordinateurs, qu'il ne faut tout simplement pas faire. C'est immoral, c'est un manque à l'éthique professionnelle, c'est également criminel. Si on fait ce genre de choses, on risque d'être poursuivi.

Pour revenir aux universités, de façon régulière, les gens essaient d'obtenir des renseignements que contiennent les dossiers des autres personnes dans les systèmes informatisés des universités. Nous pouvons convenir que c'est immoral, nous pouvons dire que c'est un manque à l'éthique professionnelle, que c'est contraire peut-être à l'accord écrit que vous avez signé en tant qu'utilisateur du système informatisé. La seule façon peut-être de le faire comprendre à certaines têtes dures pour qu'elles ne continuent pas ce genre de choses, c'est d'inclure une disposition dans le Code criminel, je suis certain qu'elle serait rarement utilisée. Néanmoins, il ne faudrait que quelques poursuites pour réveiller un peu les gens. C'est un peu comme la Loi sur la protection de la vie privée de 1974 aux États-Unis, elle contient des sanctions criminelles contre toute divulgation non autorisée des renseignements personnels. Il y a eu quelques pénalités, des poursuites en vertu de cette loi qui ont connu du succès; Il suffit de quelques poursuites pour rendre les gens plus conscients.

M. Beatty: À mon avis, le consensus est important. Je n'ai pas de difficultés, et je ne pense pas que quiconque en ait vraiment, à comprendre que des sanctions pourraient être prises contre toute personne qui «viole» une base de données.

Vous faites une suggestion nouvelle, que le propriétaire de la base a donnée, s'il n'a pas respecté les normes de sécurité adéquates, devrait être responsable. La seule situation semblable qui me vient à l'esprit relève de la Loi sur les armes à feu, si j'entrepose des armes à feu à la maison et si ma maison fait l'objet d'un vol, si quelqu'un prend ces armes que je n'ai pas convenablement cachées, je peux faire également l'objet d'accusation. Cependant, si j'ai un magasin en ville et que quelqu'un entre par effraction et vole des appareils de télévision que je prévoyais vendre, j'imagine qu'on ne peut pas faire d'accusation contre moi pour n'avoir pas installé des verrous convenables sur la porte.

Ce que vous proposez est quelque chose de relativement nouveau, en invoquant des motifs de tort causé à des tierces parties, on pourrait le faire dans le cas de la Loi sur le contrôle

[Texte]

that the real concern with this theft of the firearms is what is coming subsequently, rather than the deprivation, as far as you are concerned.

Mr. Flaherty: As I hear you reorganize my thinking for me, it becomes more and more persuasive to me. I think the argument generally is that I do not believe anybody should collect personal information unless they really need it. If a bank or a trust company or a personnel company or a loan company or a government agency has decided that they really need this data on me, and some of it could be sensitive, particularly in association with other information—or I may simply regard my age or income as sensitive, whereas somebody else might not—if they decide to keep that information, I am prepared to argue that they should have a statutory obligation to maintain that information secure and confidential and only allow it to be used for the purposes for which it was collected; if they do not do that then they should be, perhaps, criminally liable. I might as well make the case for criminal liability, since there will be plenty of people shooting holes at me from a distance if over a period of time they decide that this idea does not have a lot of merit.

Mr. Beatty: Well, you have argued over the years that we should have something extending to the private sector that is essentially now just what we have now for the government in the privacy act. In terms of appropriateness and in terms of the sanctions against an institution for inadequate data security, would it not be more appropriate to house that in a data protection act that extends to the private sector and then in the context of a law dealing with computer crime per se? I get a much broader concern, although the committee is relatively narrowly focused.

Mr. Flaherty: I am trying to respond to an invitation to talk about the privacy aspects of computer-based crime in trying to get something to say, rather than giving what I would hope to give in several years time—considerations as to how you can revise the excellent Privacy Act of 1982 and make it even more excellent.

I do generally argue, as I have in my recent work on two-way cable television and privacy, that in the current political atmosphere of North America, the private sector is better off self-regulating, and I have advocated self-regulation to protect privacy interests which would include maintaining appropriate security. I am appalled by the lack of progress in data protection in every province of this country, except Quebec. I see a possibility here, by using the criminal law, which is federal, to extend data protection in certain ways to all kinds of information systems. And if I may be mildly cynical, the mere fact that someone is talking about this will raise enough hackles that some custodians of personal information will begin to look around their shops to see if Canada signed the OECD guidelines for the protection of personal information

[Traduction]

des armes à feu en disant que ce qui est plus préoccupant, c'est ce qui suivra le vol des armes à feu, plutôt que la privation de ces armes en autant que vous êtes concerné.

M. Flaherty: Je vous entends réorganiser ma pensée, et je suis de plus en plus persuadé. De façon générale, l'argument serait celui-ci: je ne crois pas que quiconque doive faire la collecte des renseignements personnels à moins qu'il en ait vraiment besoin. Si une banque ou une fiducie ou un bureau de personnel ou un bureau de prêt ou un agent du gouvernement décidait qu'ils ont vraiment besoin de ces données me concernant, si certaines de ces données sont délicates, particulièrement en rapport avec d'autres renseignements—ou je peux tout simplement considérer mon âge ou mon revenu comme étant des sujets délicats—alors que pour d'autres ça ne l'est pas, s'ils décidaient de conserver ces renseignements, je suis prêt à prétendre qu'ils devraient avoir l'obligation statutaire de conserver à ces renseignements leur aspect sécuritaire et confidentiel et de ne pas permettre à quiconque de les utiliser autrement qu'aux fins pour lesquelles ils ont été obtenus. S'ils ne le font pas, ils pourraient être, peut-être, tenus criminellement responsables. Je suis aussi bien de soulever cette cause de responsabilité criminelle, étant donné qu'un grand nombre de personnes vont me prendre pour cible si après une certaine période, ils décident que cette idée n'est pas vraiment méritoire.

M. Beatty: Vous avez prétendu, depuis plusieurs années, qu'il faudrait inclure pour le secteur privé essentiellement ce que nous faisons maintenant dans la Loi sur la protection des renseignements personnels. Quant à leur convenance et aux sanctions prises contre toute institution qui n'a pas de mesures de sécurité adéquates pour les données, ne vaudrait-il pas mieux de mentionner dans une loi sur la protection des données qui toucherait également le secteur privé et dans le contexte d'une loi qui traiterait des crimes reliés aux ordinateurs comme tels? Mes préoccupations sont assez vastes, même si le comité se limite à relativement peu de questions.

M. Flaherty: J'essaie de répondre à une invitation de parler des aspects secrets du crime relié aux ordinateurs, j'essaie de dire quelque chose, plutôt que de donner ce que j'aimerais bien communiquer dans quelques années, sur la façon dont on pourrait réviser cette excellente loi sur la protection des renseignements personnels de 1982 et de la rendre encore plus parfaite.

Je prétends généralement, comme je l'ai fait dans un travail récent sur la télévision par câble dans les deux sens et la protection des renseignements personnels, que dans l'atmosphère politique actuelle en Amérique du Nord, le secteur privé est mieux de se réglementer lui-même. En outre, j'ai soutenu que l'auto-réglementation protégerait les intérêts des renseignements personnels et comprendrait le maintien d'une sécurité convenable. Je suis tout à fait étonné du manque de progrès qu'on fait pour protéger les données dans les provinces au pays, sauf au Québec. Il y a possibilité, en se servant du droit criminel, avec le fédéral, d'élargir la protection des données d'une certaine façon pour qu'elle englobe tous les genres de systèmes d'information. Pour être un peu cynique, le simple fait qu'une personne en parle va soulever suffisamment de

[Text]

and whether their particular operation would be in compliance with the basic principles of it.

Mr. Beatty: Moving away then from the question of mandatory levels of security to the question of violations of data bases and the violator himself, at least one jurisdiction in the United States has a mandatory reporting requirement. That is generally being resisted by some institutions, including universities, who prefer to have the option of deciding whether they want to report an individual who has broken into their data base or to deal with it through internal sanctions. Would you favour a mandatory reporting requirement on the part of institutions if their data base were violated?

Mr. Flaherty: I do not have any professional knowledge of that kind of issue. I suppose as an historian I have some knowledge of human nature, and I would be very pessimistic that you could ever make a mandatory scheme of that sort work.

Mr. Beatty: One of the other suggestions that was made the other day—and which has some appeal, frankly—was the argument that we should make the legislation we have as simple as possible. The more complex it gets, the more roadblocks are put in the way of acting and people would say: Look, the technology is very fast-changing; it is extremely complex as it is; and, by golly, if you legislate today, the law will be obsolete tomorrow.

• 1715

The argument was made the other day that we have something akin to a computer trespass law, rather than dealing with the data itself and saying that the data are sacrosanct that you would try to treat computers in much the same way as you would treat manual files. If I were to break into your office and rifle through your files, you might be able to charge me with criminal trespass or break and enter. If I were to do it in your computer using the telephone system, I appear to be immune from the law as things stand today.

Does the suggestion that you have something akin to a computer trespass law have any particular appeal to you as a possible first step in dealing with this?

Mr. Flaherty: I am very much persuaded of the desirability of simplicity, and I think the universal quality to all of this is that you are dealing with information. Whether it is microcomputers, personal computers, home computers, or large main-frame computers does not really matter. You are talking about information flowing, and only some of it is personal information. I think you basically should be saying it is unlawful to obtain access without permission to any information system; it is unlawful to disclose it and so forth.

Going specifically to your point, one of the most innovative provisions in the Swedish Data Act of 1973, which was the

[Translation]

remous pour que les gardiens des renseignements personnels commencent à voir un peu autour d'eux si le Canada a signé des directives de l'OCDE qui visent à protéger les renseignements personnels et si leur propre maison se conforme aux principes fondamentaux de ces directives.

M. Beatty: Pour nous éloigner un petit peu de la question des niveaux de sécurité obligatoires et aborder celles des violations des données de base et des responsables de ces violations, une juridiction au moins aux États-Unis a prévu le rapport obligatoire. Certaines des institutions, y compris les universités, y résistent de façon générale, elles préfèrent avoir le choix de décider si elles veulent rapporter une personne qui a violé leur base de données ou traiter de la question par voie de sanction interne. Seriez-vous en faveur de l'obligation de faire rapport pour les institutions si leur base de données est violée?

M. Flaherty: Je ne connais pas professionnellement ce genre de questions. Je suppose qu'en tant qu'historien, je connais un peu la nature humaine, et je suis très pessimiste quant à l'issue d'un projet comme celui-ci.

M. Beatty: On a fait d'autres suggestions l'autre jour, une de celles-là, je la trouve assez attrayante, c'est que nous devrions rendre la loi aussi simple que possible. Plus le sujet est complexe, plus les obstacles sont nombreux qui nous empêchent d'intervenir. Combien nous disent que, étant donné que la technologie évolue très rapidement et est déjà très complexe, la loi que vous adopterez aujourd'hui sera complètement désuète demain.

L'autre jour, quelqu'un a dit qu'il vaudrait mieux avoir une loi interdisant l'utilisation clandestine des ordinateurs, plutôt que de s'en tenir aux données elles-mêmes en affirmant qu'elles sont sacro-saintes, car à ce moment-là, vous traiteriez les ordinateurs presque comme des manuels. Si j'entraîs dans votre bureau par effraction pour consulter vos dossiers, vous pourriez m'inculper de violation de propriété ou de vol par effraction. Par contre, si je pénétrais dans vos circuits d'ordinateur au moyen du téléphone, je ne suis pas, à l'heure actuelle, passible de poursuite.

Pensez-vous que l'adoption d'une loi sur l'intrusion illicite dans les circuits informatiques serait une première étape valable pour résoudre ce problème?

M. Flaherty: Je suis convaincu de la nécessité de trouver un moyen très simple pour y parvenir et, bien sûr, le point commun de tous ces problèmes est qu'ils traitent de l'information. Que cette information soit transmise par des micro-ordinateurs, des ordinateurs personnels, des ordinateurs domestiques ou de gros ordinateurs industriels, cela a peu d'importance. Il s'agit toujours de transferts d'informations, dont une partie seulement sont des informations personnelles. À mon avis, ce que vous devriez dire, c'est que, en substance, il est illégal de pénétrer clandestinement dans un système d'information, et qu'il est illégal d'en divulguer les données.

Pour en revenir à votre question, j'aimerais signaler ici que l'une des dispositions les plus innovatrices de la loi suédoise de

[Texte]

first national provision on data protection, is the concept of data trespass, which is very close to what you have just said. The provision of the law is:

Any person who unlawfully procures access to a recording for automatic data processing or unlawfully alters or obliterates or enters such a recording in a file shall be sentenced for data trespass to a fine or to imprisonment not exceeding two years unless the offence is punishable under the penal code.

So they have had data trespass there.

I can tell you on the basis of my studies of these foreign data protection laws that the criminal sanctions are rarely used. What is important is that either someone contemplating a particular nefarious activity or the possessors of the personal information know the standards they are supposed to maintain. For example, in France the National Commission on Informatics and Freedom has issued a two-page statement giving custodians of personal information some sense of what the standards are on security that they are supposed to maintain so people know what is expected of them.

Mr. Beatty: Just one final question. I apologize to the chairman for being as lengthy as I have been, but it has been a very useful presentation that you have made.

We heard Professor Palmer talking about copyright as one means of dealing with protection of computer software. You have talked in terms of more generalized law dealing with data protection that relates to personal information. There are many specialized ways in which we could deal with the various aspects of what we refer to broadly as computer crime.

I am increasingly led to the belief that it may be that the argument in favour of computer trespass or something similar to that might be the best way to proceed, particularly in view of the difficulty of assigning a value to information. Until today, by and large the testimony that we have had has dealt with the value to institutions of information; that in itself, it was pointed out to us, is very, very difficult to evaluate. Whose value do you set on it? Do you set the value of it to the thief, the value to the institution that had it stolen from it, or whom? Or perhaps the cost of compiling the information, the cost of deprivation and so on? It is very hard to say.

You have thrown another intangible into the equation when you are dealing with personal information—potential embarrassment, for example. In terms of assigning the appropriate penalty to theft of information relating to an individual it must be very difficult to say how harsh the penalty should be when you are dealing with something similar to embarrassment or even if an individual was not embarrassed but was simply affronted by the fact that somebody had taken information that he felt belonged to him and not to anyone else. It would be very difficult, I imagine, for the courts to assess that. It may very well be that the best way for us to deal with that for the time being would be to simply say that if somebody gains

[Traduction]

1973 *Swedish Data Act*, qui était la première à avoir été adoptée dans le domaine de la protection des données, reposait sur la notion d'intrusion illicite dans les circuits informatiques, ce qui se rapproche beaucoup de ce que vous venez de dire. Cette loi stipule ainsi que:

Celui qui procure illégalement l'accès à un enregistrement d'un système de traitement des données, ou qui modifie, efface ou insère illégalement cet enregistrement dans un dossier est coupable d'intrusion illicite et passible d'une amende ou d'une peine d'emprisonnement de deux ans ou plus, à moins que l'infraction ne relève du Code pénal.

Ils ont donc dans cette loi la notion d'intrusion illicite.

J'ai étudié personnellement les lois adoptées par plusieurs pays en matière de protection des données, et je peux vous dire que les sanctions pénales qu'elles contiennent sont rarement utilisées. Ce qui est important c'est que, soit celui qui envisage de se livrer à une activité illicite, soit le possesseur de ces données personnelles, connaisse les normes qu'ils sont censés respecter. Par exemple, en France, la Commission nationale sur l'informatique et la liberté a publié à l'intention des responsables de ces données personnelles un texte de deux pages indiquant les normes de sécurité qu'ils sont censés assurer, de sorte qu'on sait ce qu'il faut attendre d'eux.

M. Beatty: Permettez-moi de vous poser une dernière question. Je m'excuse auprès du président d'être aussi long, mais votre exposé a été particulièrement intéressant.

Le professeur Palmer nous a dit que la notion de droits d'auteur pourrait être appliquée pour protéger les logiciels. Vous, vous préconisez une loi plus générale sur la protection des données, et plus précisément des données personnelles. Il existe beaucoup de mécanismes que l'on pourrait employer pour lutter contre ce que l'on appelle en général la truaquerie.

Je suis de plus en plus porté à croire que la notion d'intrusion illicite dans les circuits informatiques, ou quelque chose de semblable, serait sans doute la meilleure façon de procéder, d'autant plus qu'il est particulièrement difficile d'attribuer une valeur à ces données. Jusqu'à aujourd'hui, les témoignages que nous avons entendus traitaient généralement de la valeur de ces données pour les organismes; d'après ce qu'on nous a dit, il est très difficile de déterminer cette valeur. Vous choisirez la valeur qui aura été fixée par qui? Celle qui aura été déterminée par le voleur ou celle qui aura été déterminée par l'organisme qui aura été volé? Cette valeur représente-t-elle le coût de la compilation des données, le coût qui en résulte pour l'organisme d'en être privé, etc.? C'est très difficile à dire.

Vous avez ajouté un autre inconnu à cette équation lorsque vous avez parlé des données personnelles, qui risqueraient, par exemple, de causer un certain embarras. Je pense donc qu'il sera très difficile de déterminer la sévérité de la peine à imposer à celui qui aura volé des informations, lorsqu'il faudra tenir compte de facteur aussi abstrait que l'embarras causé à la victime ou, sinon, au simple affront que constituera, pour elle, le simple fait qu'on lui ait volé des informations qui lui appartenaient à elle et à personne d'autre. J'imagine qu'il sera très difficile pour les tribunaux d'évaluer cette sanction. En ce qui nous concerne, pour l'instant, il vaudrait peut-être mieux décréter que celui qui est coupable d'une intrusion illégale

[Text]

unauthorized access to information held in a computer then he has committed an offence. It is hard and fast and clear. It sets some sort of societal standard. We are saying society does not approve of this sort of action, and you have a legislative standard that is relatively neat and easy to deal with.

• 1720

In your opinion, would this likely be the best way for us to proceed at this point?

Mr. Flaherty: That sounds very attractive to me, the way you have described it. I was looking at the range of sanctions in some of the laws I reviewed in my written testimony; and I thought the French one ran from two to six months' imprisonment, a fine from 2,000 to 20,000 francs, or both. I think when I first wrote this testimony, that was 200,000 francs; there may have been a loss of a zero in our wonderful word processor somewhere along the way. But you can see the great range there. I think, since it is very unlikely anybody is very frequently going to be prosecuted, the minimum range we usually put on these sorts of things would be fine.

Mr. Beatty: Thank you very much.

Thank you, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you.

Professor Flaherty, you have indicated in your written notes to us that you are presently engaged in a study over a period of some four years, I guess, and that it is not complete yet. It will be completed next year. Does your study, in fact, cover the kind of matter we have before this committee?

Mr. Flaherty: It covers it from the point of view of the extent to which there are criminal sanctions in data protection laws. I have reviewed for you in my written testimony the extent to which there are criminal sanctions; and basically, almost all of them have criminal sanctions against abuse of personal information, which I have usually thought of as part of the privacy and security problem rather than as part of the computer-based crime problem. But that is simply a reflection of my education and how I have learned to think about this rather than any sort of reason that you should not be thinking about it in the present context of the responsibilities of your subcommittee.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Now, in your study of the situation in Europe—I guess that includes the United States and Canada as well—how far behind are we in Canada compared to Europe, in your view?

Mr. Flaherty: I can only talk in terms of how Europeans regulate access to and disclosure of personal information; and generally speaking—and especially before the privacy legislation of 1982 in this country was actually proclaimed and made workable—they have much more progressive systems on the continent of Europe in most countries than we have in

[Translation]

dans des circuits informatiques est coupable d'une infraction. À mon avis, c'est clair et net. Cela permet d'établir une certaine norme sociétale. On déclare en effet que la société n'approuve pas ce type d'actes, et la norme que vous établissez par voie législative est relativement claire et facile à faire respecter.

À votre avis, pensez-vous que ce serait, pour l'instant, la meilleure façon de procéder?

M. Flaherty: De la façon dont vous le décrivez, cela me paraît très séduisant. J'essayais de me souvenir de la gamme de sanctions que prévoyaient les textes législatifs que j'ai passés en revue dans ma déclaration; en France, la peine d'emprisonnement peut aller de 2 à 6 mois, l'amende de 2,000 à 20,000 francs, et la sanction peut prévoir les deux. Si je me souviens bien, lorsque j'ai rédigé cet exposé, il s'agissait de 200,000 francs; notre ordinateur a peut-être laissé tomber un zéro en cours de route! Cependant, cela vous donne un ordre de grandeur. Étant donné qu'il est fort peu probable que la même personne soit fréquemment poursuivie, la sanction minimum que nous imposons généralement dans ce genre de cas devrait suffire.

M. Beatty: Merci beaucoup.

Merci, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci.

Professeur Flaherty, vous avez indiqué, dans votre mémoire, que vous faisiez actuellement une étude entamée il y a trois ans et qui devrait être terminée l'année prochaine. Cette étude porte-t-elle sur les genres de questions dont est saisi notre comité?

M. Flaherty: Oui pour ce qui est de la question de savoir dans quelle mesure les lois sur la protection des données sont assorties de dispositions pénales. C'est un sujet que j'ai abordé dans mon mémoire et, si je peux résumer, pratiquement toutes ces lois contiennent des dispositions pénales contre l'utilisation abusive des renseignements personnels, ce qui, à mon avis, participe davantage du problème de la protection des renseignements personnels que de celui de la trauandique. Mais c'est peut-être une déformation de mon éducation et de mon propre mode de pensée, et ce n'est pas une raison pour que vous n'étudiez pas cette question au sein de votre sous-comité.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez fait une étude sur les pays européens, et également sur les États-Unis et le Canada, et j'aimerais savoir dans quelle mesure le Canada est en retard par rapport à l'Europe?

M. Flaherty: Je peux simplement vous dire ce que font les Européens pour réglementer l'utilisation et la divulgation des renseignements personnels; de façon générale et c'était surtout valable avant la promulgation, en 1982, de notre Loi sur la protection des renseignements personnels, les pays européens ont un système beaucoup plus progressiste qu'au Canada pour

[Texte]

Canada on the issues of controlling unauthorized access to and disclosure of personal information and the maintenance of appropriate security procedures for personal information. In other words, the West Germans, the Swedes, and the French, in particular, have bureaucracies whose job it is, often in both the public and private sectors... In fact, in those three countries, in both the public and private sectors, for any type of personal information system, they establish by national or federal statute who should have access to information, what could be done with it. In fact, in Sweden there is a licensing scheme. So North America—the United States and Canada—are generally behind those regulatory schemes in Europe.

Now, the danger is that you will apply my generalization to the whole field of computer crime, much of which deals with non-personal information; and I simply do not know much about that subject.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Your paper seems to indicate you are dwelling particularly on the criminal aspects of it in terms of penalties and bringing notice to the community and to people generally of this whole question of computer crime or computer abuse. But at the same time, you are talking about guidelines and regulations for the security in computer systems and this kind of thing.

Now, where do you draw the line between one and the other? Certainly in the Criminal Code you do not have a list of guidelines or regulations flowing from it; rather, you have the case law on the provisions of the Criminal Code itself. Do you see a correlation between the two or do you feel there should not only be an amendment to the Criminal Code but also a special act?

Mr. Flaherty: I would have to distinguish here between the three parts of my focus. I think there ought to be criminal sanctions concerning unauthorized access to personal information and unauthorized disclosure of personal information. I am less sanguine—and I indicated that during my discussions with Mr. Beatty—that you can fashion criminal sanctions for people who do not maintain appropriate security standards. That would be unusual.

• 1725

I can hardly claim to think as a Canadian on this particular issue, and I have trouble deciding whether the French, the Swedish, the American, or whatever model would be most appropriate—whether it ought to be in regulations, in guidelines. We have problems of comparative law here, between the civil and the common law system of anglo-saxon countries.

I really do not think I can be definitive for you in terms of what we ought to do in the federal Criminal Code versus elsewhere, partly because I am trying to fulfil a variety of motives in both testifying to you and in trying to make these kinds of arguments. That is, I think computer-based crime is not a good thing; you ought to do something about it. I am trying to remind you, as I think you already know, that there is

[Traduction]

ce qui est de contrôler l'utilisation et la divulgation clandestines des renseignements personnels et pour ce qui est de l'adoption de procédures de sécurité appropriées relativement à ces renseignements personnels. En d'autres termes, les Allemands de l'ouest, les Suédois et les Français surtout, ont des bureaucraties dont le rôle, et c'est valable aussi bien pour le secteur privé que pour le secteur public... En fait, dans ces trois pays, une loi nationale définit ceux qui pourront avoir accès aux renseignements appartenant à n'importe quel circuit informatique personnel, et ce dans le secteur public comme dans le secteur privé. En fait, il y a même en Suède un système d'octroi de permis. On peut donc en conclure que l'Amérique du Nord, c'est-à-dire les États-Unis et le Canada, sont généralement en retard par rapport à ces schémas de réglementation européens.

Cependant, il y a un danger à appliquer la généralisation que je viens de faire à toute la question de la truandique, dont la majeure partie concerne des renseignements non personnels; là-dessus, je ne peux pas vous dire grand-chose,

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans votre mémoire, vous semblez insister tout particulièrement sur les aspects criminels de la truandique, puisque vous parlez essentiellement des sanctions possibles. Vous parlez également des directives et règlements permettant d'assurer la sécurité des circuits informatiques.

Où tracez-vous la ligne de démarcation? Le Code criminel ne comporte pas une liste de directives ou de règlements à cet égard; vous devez plutôt vous baser sur la jurisprudence découlant des dispositions du Code criminel. Pensez-vous qu'il existe une corrélation entre les deux ou bien estimez-vous qu'il faudrait non seulement modifier le Code criminel mais aussi adopter une loi spéciale?

M. Flaherty: Permettez-moi de faire une distinction ici entre les trois parties de mon exposé. À mon avis, il faut prévoir des sanctions en cas d'utilisation et de divulgation illicites de renseignements personnels. Par contre, et je l'ai déjà indiqué tout à l'heure à M. Beatty, je ne pense pas que l'on puisse formuler des sanctions contre ceux qui ne respectent pas des normes de sécurité appropriées. Cela serait inhabituel.

Je ne peux guère prétendre raisonner en Canadien à ce propos, et j'ai du mal à décider si le modèle français, suédois ou américain conviendrait le mieux et s'il devrait être consacré par des règlements ou des lignes directrices. Des problèmes de droit comparatif se posent dans ce cas-ci et plus précisément entre le droit civil et le *common law* des pays anglo-saxons.

Je ne crois pas pouvoir vous dire s'il vaudrait mieux modifier le Code criminel fédéral ou adopter une autre démarche, car j'essaie de répondre à plusieurs motifs en comparaisant devant vous, tout en essayant de présenter des arguments. Cela dit, je pense que la truandique devrait être réprimée d'une façon ou d'une autre. Rappelez-vous, et je pense que vous le savez déjà, que de nombreux renseignements personnels sont en jeu et que

[Text]

a lot of personal information at stake, and that the interests not only of the data owners ought to be protected but also the data subjects. Because I have only been thinking intensively about the criminal side of this since Friday morning when I got your invitation, I am not willing to go to the depth in terms of supporting these recommendations. I simply think there are human rights aspects of computer-based crime that you ought to think about.

I should also make a point that when you are looking at this problem strictly in the human rights context, you start with a straightforward problem of protecting privacy, or whatever it is called in a particular country, and the criminal sanctions look rather small in that context. They are not a central part, for example, of my study. My study finds it is much more important to have inspections carried out by the data protectors in West Germany and France, to check on security regimes. The West German data protectors go in and take over the computer system of a government agency, for example, and test the security regimes, and then give them recommendations on how to improve it. So that is where the need for criminal sanctions gets a little far afield.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I get the impression from your comments that your primary focus is on the right to privacy, but there is a feeling of frustration in that the privacy legislation does not appear to be working the way it ought to be. As you said yourself, there are only a few cases that come before the courts, and in those cases the results are not particularly satisfactory. You have indicated quite a degree of frustration in this regard. Do I have the impression rightfully that what you are really suggesting is that maybe the criminal law could be used as a backup to these other statutes that do not appear to be working? Would that be a fair statement to make?

Mr. Flaherty: Exactly, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You mentioned in particular the Bank Act, for one. Are you suggesting also that there should be provisions in many many federal statutes—and I do not propose to enumerate them in any way—concerning privacy and also concerning the security of information?

Mr. Flaherty: Yes, Mr. Chairman. In one of the material sources I cited to you, in fact in the Krever commission report on the confidentiality of health information in Ontario, in one of the appendices he and his staff reviewed all the health-related statutes in Ontario which include some provision on confidentiality. So if we were to do a listing of all the federal statutes that had something to say about the confidentiality of personal information, we would find that there is usually something in a statute. There happens to be nothing in the federal Bank Act, which is a particularly outrageous instance as far as I am concerned.

[Translation]

non seulement les intérêts des propriétaires de données devraient être protégés, mais également les données elles-mêmes. Depuis vendredi matin, date à laquelle j'ai reçu votre invitation, je ne fais que penser au côté criminel de cette activité, et c'est la raison pour laquelle je ne désire pas accorder un appui inconditionnel à ces recommandations. Je pense simplement que les délits informatiques présentent certains aspects ayant trait aux droits de la personne et que vous devriez y réfléchir.

Je voudrais également faire remarquer que si vous abordez ce problème strictement du point de vue des droits de la personne, le problème qui vient immédiatement à l'esprit est de protéger la vie privée des individus en question, ou quel que soit le terme utilisé dans un pays en particulier, ce qui rend les sanctions pénales prises peu sévères. Par exemple, je ne leur ai pas accordé une place importante dans mon étude. D'après l'étude que j'ai effectuée, il est beaucoup plus important de faire effectuer des inspections par les inspecteurs de données en Allemagne de l'Ouest et en France, inspecteurs chargés de vérifier les systèmes de sécurité. Les inspecteurs ouest-allemands vérifient les systèmes de sécurité des systèmes informatisés d'un organisme gouvernemental, par exemple, et proposent ensuite aux dirigeants de cet organisme des recommandations sur les moyens de l'améliorer. On s'éloigne donc beaucoup avec cette histoire de sanctions pénales.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Les observations que vous faites me donnent à penser que vous accordez une importance prioritaire au respect de la vie privée des individus, mais qu'il vient s'y ajouter un sentiment de frustration dans la mesure où la législation du droit à la vie privée ne semble pas avoir les résultats escomptés. Comme vous l'avez dit vous-même, seules quelques affaires parviennent aux tribunaux et encore faut-il noter que les résultats ne sont pas particulièrement satisfaisants. Vous avez fait part de votre frustration à cet égard. Ai-je raison de penser que vous suggérez en fait de recourir au droit pénal lorsque les autres textes de loi ne semblent pas donner les résultats voulus? Est-ce ce que vous pensez?

M. Flaherty: Exactement, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez fait en particulier allusion à la Loi sur les banques. Proposez-vous de rajouter des dispositions à de nombreuses lois fédérales, et je n'entends pas les énumérer toutes, portant sur le respect des libertés individuelles et sur la sécurité de l'information?

M. Flaherty: Oui, monsieur le président. Dans un des documents que j'ai cités, à savoir, le rapport de la Commission Krever sur le caractère confidentiel des renseignements sur l'état de santé des particuliers en Ontario, une des annexes de ce rapport fait état de toutes les lois ontariennes ayant un rapport quelconque avec la santé et qui comportent des dispositions sur le caractère confidentiel de ces renseignements. Par conséquent, si nous devons citer toutes les lois fédérales comportant une disposition sur le caractère confidentiel de renseignements personnels, nous constaterions qu'en général cette disposition existe. Or, il n'existe aucune disposi-

[Texte]

So I think there ought to be in any specific piece of federal or provincial legislation, whether for the public or the private sector, there ought to be a fairly simply worded stipulation that, if personal information is collected and stored, it ought to be kept confidential. And subject to the problems of knowing how to formulate such a criminal sanction, I suppose I think it would be desirable to also have statutorily mandated security, even if it was only at the level of telling custodians of personal information that they had a statutory responsibility, subject to potential criminal sanctions, to maintain proper security for personal information in their custody.

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): So really what you are saying is that we need both the statute law and the criminal law as a backup. I note on page 2 of your statement where at the bottom it says:

Unauthorized disclosure of personal information is often not an offense.

—and this, of course, is the great concern that you have. You go on:

At the same time it must be recognized that designing and drafting a criminal statute to regulate aspects of invasion of privacy may be a tricky matter as compared to the drafting of protections for data with commercial value.

I would like you to comment on that statement, if you would. It is...

• 1730

Mr. Flaherty: I am glad I cut the subsequent sentence out of this draft or you would have even more things to play with. I had some problems with that sentence; there was a sentence after it that I had even more problems with, so I cut that out. So you put your hand on a mild Achilles' heel.

I simply wanted to indicate, since I come out of a university law school, that I am aware of the problems of, first, using the criminal law in this area; second, of the philosophical debates over whether the criminal law is really going to be effective in teaching people morality; and third, about the drafting problems, the technical issues. But I can see from the testimony you received from the Department of Justice that there is no shortage of technical experts around who presumably can take simple language and—if I may say so with tongue in cheek—turn it into complex statutes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, as a committee I think we are looking for all the help we can get with regard to potential drafting, not only of an amendment to the Criminal Code, but also to special legislation concerning the matter before us. If you can help us in any way with regard to that we would be very appreciative of it.

[Traduction]

tion de ce genre dans la Loi fédérale sur les banques, ce qui est particulièrement scandaleux à mon avis.

Donc, chaque texte de loi fédérale ou provinciale destiné soit au secteur public, soit au secteur privé, devrait comporter un article libellé en termes clairs, selon lequel toute information personnelle stockée devrait être confidentielle. Quant à l'établissement des sanctions pénales, je suppose qu'il serait souhaitable d'y introduire un autre élément de sécurité, même si celui-ci ne consiste qu'à informer les agents protecteurs de renseignements personnels que, sous réserve d'éventuelles sanctions pénales, la loi les rend responsables de la sécurité des renseignements personnels qu'ils ont sous leur garde.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous dites donc en réalité que nous devons pouvoir recourir aux textes législatifs et au droit pénal si le besoin s'en faisait sentir. Je vois que vous dites à la page 2 de votre déclaration, vers le bas de la page, ceci:

La divulgation indue de renseignements personnels ne constitue souvent pas une infraction.

... et cela est manifestement ce qui vous préoccupe le plus. Vous poursuivez en ces termes:

Mais il faut également reconnaître que l'élaboration d'une loi pénale réglementant certains cas d'atteinte à la vie privée peut se révéler plus difficile que l'élaboration de mesures protégeant les données ayant une valeur commerciale.

Je voudrais que vous commentiez cette observation.

M. Flaherty: Je suis content d'avoir supprimé la phrase qui suivait sinon vous auriez eu encore plus de sujets de discussion. Cette phrase me gênait et celle qui suivait encore plus, si bien que j'ai supprimé tout cela. Vous avez donc découvert mon talon d'Achille.

Je voulais simplement faire remarquer, puisque je sors d'une faculté de droit, que je suis conscient d'abord des problèmes inhérents au recours au droit pénal dans ce domaine, ensuite des débats d'idées qui portent sur la question de savoir si le droit pénal parvient à inculquer des principes de moralité à certaines personnes et enfin des problèmes d'élaboration à savoir, les points de détail. Mais je constate, d'après les témoignages que vous avez eus du ministère de la Justice, que les experts techniques ne manquent pas, experts qui peuvent, si vous me permettez cette remarque amusante, tourner quelque chose de simple en quelque chose d'extrêmement compliqué.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je crois que ce Comité cherche avant tout à obtenir toute l'aide qu'il peut en matière d'élaboration d'un texte législatif, qu'il s'agisse d'une modification qui soit apportée au Code criminel ou de tout texte législatif spécial portant sur le sujet à l'étude. Nous vous serions extrêmement reconnaissants si vous pouviez nous aider de quelle que façon que ce soit.

[Text]

I would like to turn to another aspect of your report, where you state on page 4, once again at the bottom of the page:

I think it is significant and relevant to your deliberations that the Canadian federal Privacy Act of 1982 does not contain similar measures; . . .

And this had to do with the security standards, I assume.

Mr. Flaherty: Yes, and also . . .

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): And do you have some suggestions as to what this Privacy Act should contain in order to meet the security standards you are speaking of?

Mr. Flaherty: I must admit, Mr. Chairman, I am still waiting for the chance to celebrate the proclamation of the statute and the appointment of a privacy and information commissioner before I start criticizing the legislation. I am delighted there is a built-in statutory review by the Standing Committee on Justice and Legal Affairs, I presume, of the legislation, which will occur within several years.

I must admit that the deficiencies of Part IV of the Canadian Human Rights Act were so great that I am still feeling this was a great accomplishment, to pass the Privacy Act, particularly because it is coupled with access to information. I was surprised when I looked at it—in this particular area of the existence of criminal sanctions and the mandating of security standards—to discover there was nothing in the legislation on that point.

I know, as you know, something about the fact that there are security standards in federal government departments and that the RCMP has something to do with them. How good are they? Is that the way it should be done? I have done studies for Statistics Canada. I know they have good security, to the extent that as a layperson I can measure that kind of thing. But I also remember the tales in the late 1970s of people being able to gain unauthorized access to Revenue Canada statistics to obtain the tax return of, say, Joe Clark, for example.

The Privacy Act is a very innovative statute because it is coupled with access to information. By international standards it is not particularly innovative, as grateful as I am to have it, and I was surprised to find, in comparison to these other pieces of legislation, that it had these lacuna. On the other hand, as I have already indicated, it is clear that the criminal sanctions under the European and American legislation have rarely been used. How can I, or you, measure what has been the effect of the existence of these sanctions? It is very difficult to measure. I think they are desirable, particularly in raising peoples' consciousness and establishing the fact that you should not unlawfully disclose personal information from somebody else's data bank if you are an employee of that data bank.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): In regard to the United States Privacy Act, you

[Translation]

Je voudrais maintenant passer à un autre aspect de votre rapport et je cite le bas de la page 4:

Je crois qu'il est important de noter que la Loi fédérale sur la protection de la vie privée de 1982 ne renferme pas de mesures semblables; . . .

Vous faites allusion aux normes de sécurité, je suppose.

M. Flaherty: Oui, et également . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Et avez-vous des dispositions à proposer sur le respect des normes de sécurité auxquelles vous faites allusion?

M. Flaherty: Je dois admettre, monsieur le président, que j'attends impatiemment l'occasion de célébrer la proclamation de la loi ainsi que la nomination d'un Commissaire à l'information avant de me mettre à critiquer la loi. Je suis ravi que la loi prévoit une révision du texte législatif par le Comité permanent de la Justice et des questions juridiques dans quelques années.

J'avoue que les lacunes que présentaient la Partie IV de la Loi canadienne sur les droits de la personne étaient si manifestes que je continue de penser que l'adoption de cette Loi sur la protection de la vie privée a été un événement majeur surtout qu'elle renferme des dispositions sur l'accès à l'information. Lorsque je l'ai parcourue, j'ai été surpris de découvrir, dans le domaine des sanctions pénales et des normes de sécurité, que la loi ne renfermait rien sur ce point.

Je sais tout comme vous qu'elle renferme des normes de sécurité s'appliquant aux ministères du gouvernement fédéral et que la GRC possède un droit d'intervention en la matière. Sont-elles vraiment efficaces? Est-ce ainsi qu'il faille s'y prendre? J'ai effectué des études pour le compte de Statistique Canada. Je sais que le système de sécurité mis en place est efficace dans la mesure où je puis en juger en tant que profane. Mais je me souviens également des histoires qui circulaient à la fin des années 1970 sur ceux qui pouvaient avoir accès, sans y être autorisés, aux statistiques du ministère du Revenu en vue d'obtenir, par exemple, la déclaration d'impôt de Joe Clark.

La Loi sur la protection des renseignements personnels est un texte législatif très novateur dans la mesure où s'y ajoutent des dispositions sur l'accès à l'information. Elle n'est pas très originale par rapport aux normes internationales, bien que je sois reconnaissant qu'elle existe, et j'ai été surpris de constater, lorsque j'ai procédé à une comparaison de ces autres textes législatifs, que ce genre de lacune existait. Par contre, comme je l'ai déjà dit, il est manifeste qu'on a rarement eu recours aux sanctions pénales prévues par la législation européenne et américaine. Dans ce cas, comment peut-on évaluer les conséquences que l'existence de ces sanctions a entraînées? La tâche n'est pas facile. Je crois qu'elles sont souhaitables en vue de sensibiliser les gens au fait qu'on ne peut pas divulguer illicitement des renseignements personnels tirés de la banque de données d'un tiers si l'on est employé de cette banque de données.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): En ce qui concerne la Loi américaine sur la

[Texte]

make a statement that the statute requires federal agencies to establish security standards, and then you go on to say that . . . I guess it is Section 10 of that particular act, which is on page 5 of your statement. Do you feel this is something that should be contained in the Canadian act?

Mr. Flaherty: I think that would be a good example of the kind of provision you could put into a computer crime law in this country.

• 1735

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Now, I note on page 7, at the top, you have indicated there are certain recommendations on guidelines governing the protection of privacy and transport or flow of personal data, and that all the OECD countries had signed except Canada, Australia and Ireland—or Iceland.

Mr. Flaherty: I think it is Ireland, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I thought it probably should be Ireland, but it says Iceland. Do you have any reasons to present to us as to why Canada—or Australia, for that matter—would not wish to sign?

Mr. Flaherty: Despite being an academic and having some reputation for candour, Mr. Chairman, I do not think that is the kind of issue I want to speculate about, particularly because there are some private signs of the Canadian federal government's beginning to mobilize its extraordinary forces to consider signing these guidelines. I do think it is an embarrassment for Canadians who work in this area that Canada participated in the formulation of the guidelines and now should be very much bringing up the rear end of those who become signatories to it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you think it has anything to do with our Freedom of Information Act or our Right to Privacy Act?

Mr. Flaherty: I think it probably has more to do with federal-provincial relations, Mr. Chairman, and the needs of our private sector, because the OECD guidelines are designed to apply to both the public and private sectors, as I recall. There is also this very sensitive issue of transport or data flows, which Canada and the United States are totally unprepared to deal with vis-à-vis continental European nations and the United Kingdom.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have led right into the next question I was going to ask you, and that is this: You have suggested Quebec is the only province of Canada that has really done something about data protection in particular. I am wondering to what extent you feel the provinces and the federal government should get together on one of their agendas to consider this whole matter of prime importance, not only for the federal government but for the provinces as well.

[Traduction]

protection de la vie privée, vous dites qu'elle oblige les organismes fédéraux à établir certaines normes de sécurité; je crois qu'il s'agit de l'article 10 de cette loi qui figure à la page 5 de votre exposé. Pensez-vous que cette disposition devrait figurer dans la législation canadienne?

M. Flaherty: Je pense effectivement que ce serait un bon exemple du genre de disposition qui pourrait figurer dans une loi régissant les délits informatiques au Canada.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Tout en haut de la page 7, vous formulez un certain nombre de recommandations sous forme de directives pour la protection de la vie privée et la circulation des données personnelles. Je constate, en particulier, que tous les pays de l'OCDE ont signé cette entente, à l'exception du Canada, de l'Australie, de l'Irlande, ou plutôt que de l'Islande. Je crois que c'est bien l'Irlande, monsieur le président.

M. Flaherty: Il s'agit bien de l'Irlande, selon moi.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui, je pensais qu'il s'agissait probablement de l'Irlande, mais c'est écrit Islande. Le Canada, et l'Australie aussi, d'ailleurs, a-t-il des raisons de ne pas signer?

M. Flaherty: Les universités ont souvent une réputation de candeur, monsieur le président, mais malgré cela, j'hésiterais à commenter cet aspect de la situation, surtout étant donné que le gouvernement fédéral canadien aurait récemment entrepris de mobiliser ses forces extraordinaires pour envisager de signer ces directives. Cela dit, les Canadiens qui s'intéressent à cette question éprouvent une certaine honte puisque le Canada après avoir participé à la formulation de ces directives est un des derniers pays à signer l'entente.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Est-ce que cela aurait quelque chose à voir avec notre Loi sur la liberté d'information ou notre Loi sur la protection de la vie privée?

M. Flaherty: Je crois que c'est plutôt une affaire de relations fédérales-provinciales, monsieur le président. Il faut également tenir compte de notre secteur privé parce que les directives de l'OCDE doivent s'appliquer à la fois aux secteurs publics et privés, si je me souviens bien. Il y a également ce problème particulièrement délicat de la circulation des données sur lequel le Canada et les États-Unis sont très loin de se mettre d'accord avec les nations de l'Europe continentale et le Royaume-Uni.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous venez de toucher à la question suivante que j'allais vous poser: vous dites que le Québec est la seule province du Canada qui ait vraiment pris des mesures pour la protection des données, en particulier. Je me demande dans quelle mesure les provinces et le gouvernement fédéral ne devraient pas se réunir pour discuter officiellement de cette affaire particulièrement cruciale, pas seulement pour le gouvernement fédéral, mais également pour les provinces.

[Text]

Mr. Flaherty: Are you talking about data protection here, Mr. Chairman, or computer-based crime legislation?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I am talking about both, because you have indicated you want a back-up from the federal system, which would be basically, as I get it, an amendment to the Criminal Code and certain other federal statutes. But at the same time, you are talking about the provinces having certain responsibilities and powers under Section 92 of the British North America Act, which would give them the rights to pass legislation in a similar vein, I suppose, for their own particular protection.

Mr. Flaherty: I certainly think any kind of possible co-operation with the provinces to promote legislation on computer-related crime is very desirable. I am not so sure it is terribly necessary with respect to data protection. I suspect you are a resident of Ontario, Mr. Chairman, and you probably know we had the Williams commission on individual privacy and freedom of information, which spent several million dollars of our money to come up with what I regard as a distinguished series of recommendations. I leave it to someone with your background to know how you encourage politicians who have majority government to act on these kinds of recommendations.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose we can hope.

Mr. Beatty, do you have any further questions?

Mr. Beatty: No, I have not. I might add though, Mr. Chairman, that I think Professor Flaherty's contribution is a very valuable one. I think we should apologize to him for the short notice of his being here. We are unfortunately in very tight time constraints. But the issues he has introduced have been very helpful to us and I think will help to focus our deliberations.

Mr. Flaherty: Thank you very much.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you, Professor Flaherty, for appearing before us. I find your paper very comprehensive, indeed, and I will look forward to reading it more thoroughly. I had skimmed through it and read some parts of it, but I have not really had an opportunity to digest it in its full content. It may be that on a subsequent occasion we may want to hear from you further. In the meantime, if you have any further suggestions to make, I am sure the committee would be most interested in hearing from you again. Thank you very much for coming today.

Mr. Flaherty: Thank you, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): At the next meeting the subcommittee will resume consideration of its order of reference on Wednesday, May 11, 1983, at 3.30 p.m. in the same room. At that time Mr. Frank Spitzer, a consultant from Toronto, and Mr.

[Translation]

M. Flaherty: Monsieur le président, parlez-vous de la protection des données ou bien de la législation sur les crimes informatiques?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Les deux, puisque vous nous avez dit que vous recherchiez l'appui du système fédéral, principalement sous forme d'un amendement au Code criminel et à certains autres statuts fédéraux. En même temps, vous parlez des responsabilités des provinces et de leurs pouvoirs dans le cadre de l'article 92 de l'Acte de l'Amérique du Nord britannique; apparemment, cela leur donnerait le droit d'adopter des lois comparables pour leur propre protection.

M. Flaherty: À mon avis, toute forme de collaboration entre les provinces et le gouvernement fédéral pour légiférer dans le domaine du crime informatique est excessivement souhaitable. Je ne suis pas aussi certain de la nécessité d'adopter des lois pour la protection des données. Monsieur le président, vous résidez probablement en Ontario, et vous devez être au courant des travaux de la Commission Williams sur la vie privée des particuliers et la liberté d'information; après avoir dépensé plusieurs millions de nos dollars, cette commission a fini par produire une série de recommandations qui me semblent très distinguées. Maintenant, c'est plutôt à vous de trouver le moyen d'encourager les hommes politiques au pouvoir à donner suite à ces recommandations.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'imagine que nous pouvons espérer?

Monsieur Beatty, avez-vous d'autres questions?

M. Beatty: Non, je n'en ai plus. Toutefois, monsieur le président, je tiens à dire à quel point les opinions exprimées par M. Flaherty m'ont semblé précieuses. Nous avons de bonnes raisons de nous excuser de l'avoir invité si tard à assister à cette séance. Nous avons un calendrier particulièrement serré. Cela dit, les questions qu'il a soulevées avec nous nous seront très utiles et devraient nous aider à mieux orienter nos délibérations.

M. Flaherty: Merci beaucoup.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci, professeur Flaherty, de vous être rendu à notre invitation. Votre exposé me semble très exhaustif; j'ai d'ailleurs l'intention de le lire à tête reposée. Je l'ai déjà parcouru en diagonale, j'en ai lu des passages, mais je n'ai pas encore eu le temps de bien assimiler l'ensemble. Il est fort possible que nous vous demandions de revenir à un moment donné. En attendant, si vous avez des suggestions à nous faire, je suis certain que nous les accueillerons toujours avec plaisir. Merci d'être venu aujourd'hui.

M. Flaherty: Merci, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À sa prochaine séance, le sous-comité reprendra l'étude de son mandat. La prochaine séance est prévue pour le mercredi 11 mai 1983 à 15h30 dans la même pièce. Nous recevrons alors M. Frank Pitzer, un expert de Toronto, ainsi que M. Marvin Gertleman, du Conseil national de recherches.

[*Texte*]

Morvin Gentleman of the National Research Council will be
before us as witnesses.

The meeting is adjourned.

[*Traduction*]

La séance est levée.

Also 2d 2a
26
27

APPENDIX "COMP-1"

Testimony of David H. Flaherty on the Privacy Implications of Computer Crime, for the Canadian House of Commons, Standing Committee on Justice and Legal Affairs, Subcommittee on Computer Crime, Ottawa, May 3, 1983.

My name is David H. Flaherty. I am a professor of history and law at the University of Western Ontario in London. I welcome this opportunity to testify before the Subcommittee on the implications of computer crime for personal privacy.

Perhaps I can begin with some background about my involvement with privacy-related matters. I have worked on aspects of privacy since I was introduced to the subject by Professor Alan F. Westin at Columbia University in 1964. My first book was an examination of the concept of personal privacy as it existed in seventeenth and eighteenth-century America.¹

Since 1974 I have been directly involved in studying contemporary problems of data protection in Western Europe and North America. My 1979 book, Privacy and Government Data Banks. An International Perspective, looked at, in five countries, the problems of balancing the conflicting interests involved in the collection and use of personal information held by government agencies for research and statistical purposes.²

Currently, I am the principal investigator of a three-year (1981-84) research project on "Data Protection Compared: an international perspective." In essence, I am taking a critical look at how laws for privacy and data protection are working in practice in the public sector (and primarily at the national level) in the United States, Canada, the Federal Republic of Germany, France, Sweden, and the United Kingdom. My research is funded by the Ford Foundation and the Social Sciences and Humanities Research Council of Canada. I have also recently completed a study of the privacy implications of two-way cable television services for the Ontario Ministry of Transportation and Communications.

I received your invitation to testify on Friday, April 29, hence what you have before you is a product of a weekend's reflection by a person who is in no way an expert on computer-based crime. What I can offer you are some thoughts about the interrelationships among such criminal activities, the protection of personal privacy, and the need for security in computer systems. In particular, I wish to draw your attention to the dangers of invasion of personal privacy through computer-based crime and to suggest the desirability of including protections for privacy in legislation to control computer abuse.

I will admit that I have not usually worried about the protection of privacy in the context of the debate over computer-based crime, which I now recognize is a failure of perception on my part. I take comfort in the fact that a recent legislative reference manual on computer crime prepared for the U.S. Department of Justice devotes one of its four chapters to "the privacy and security aspects of computer-related crime,"³ which is the subject matter of my testimony.

1. Privacy and Security Issues in Computer-based Crime

I would like to review the arguments for and against giving serious consideration to using any new criminal laws on computer-related crime to further reinforce existing protections for the privacy of the individual in both the public and private sectors. Although it is probably true that the vast bulk of data in automated information systems does not concern directly-identifiable individuals, clearly a great deal of personal information is stored in computers and its protection raises a number of privacy issues. Thus what I have to say only relates to personal information in computer-based systems, much of which can be sensitive, as in medical, financial, tax, criminal justice, and banking systems. Unauthorized access to, unauthorized disclosure of, and/or theft of such personal data clearly poses considerable challenges for the protection of privacy.

It is arguable that citizens in the final analysis should enjoy the protection of the criminal law for certain aspects of their privacy interests in personal data. In a similar vein legislation to control computer-based crime should also mandate protection of the confidentiality of personal information stored in automated information systems. For example, the theft of personal information for whatever purposes, including illicit gain and invasion of privacy, could be well and better regulated by such legislation than is currently the case. The interests harmed in such episodes are not only those of the owners of the data but also the persons involved. If it is not already the case, it should be a criminal offense to obtain unauthorized access to such personal information systems as government data banks, health and personnel records, and confidential research data.

In addition to unauthorized access and unauthorized disclosure, legislation to control computer-related crime should also mandate security requirements and standards in order to protect the privacy interests of individuals, especially in the private sector. Such a criminal law would not only protect the property interests of the data owner against the indiscrete or malicious employee, but also the privacy interests of persons recorded in such an information system. As Mr. Justice Krever noted in his outstanding study of the confidentiality of health information, "the truth

is... that the greatest security risk is to be found, not in the system's hardware or software, but rather in the persons involved in the system."⁴

It seems evident that certain problems exist with the laws concerning the protection of personal information in automated systems, especially with respect to the risks of unauthorized penetration and use of data. Many federal and provincial statutes already prohibit certain types of disclosure and sometimes make it a criminal offense to do so.⁵ This is much less frequently the case in the private sector. But current statutory protections of this type in Canada and the United States appear to be of a piecemeal character, of recent vintage, few in number, and relatively unused for criminal prosecutions.⁶ Unauthorized disclosure of personal information is often not an offense. At the same time it must be recognized that designing and drafting a criminal statute to regulate aspects of invasion of privacy may be a tricky matter as compared to the crafting of protections for data with commercial value.⁷

2. Problems of Privacy and Security in Automated Information Systems

My colleague Neil Vidmar and I recently directed a survey involving more than two hundred in-depth interviews among a random sample of households in London, Ontario in order to ascertain attitudes towards personal privacy. Although the survey has not yet been released by our government clients, I feel free to state that it revealed surprisingly high levels of expression of concern for the protection of privacy among the sample, which is in agreement with the limited amount of survey data previously available for Canada. Ninety percent of respondents said protecting privacy was important or very important. In comparison to six other social and economic issues, protection of privacy was rated as somewhat less important than controlling inflation, unemployment and crime, but just barely. It was rated as more important than stopping the spread of nuclear weapons, strikes, and improving Quebec/English-Canada relations. In comparison with six other human rights and social issues, protecting privacy was rated as the most important. These results surprised me as a privacy advocate; I offer them to you as strong evidence of continuing concern for the protection of privacy among the Canadian population. Although this committee deserves congratulations for its role in passing the federal Privacy Act of 1982, only Quebec among Canadian provinces has counterpart data protection legislation for the public sector; the private sector is almost completely unregulated.⁸

I would simply remind you that many current possibilities for stealing personal information have privacy implications, which are not covered by such rules as exist against wiretapping, for example. The advent of two-way cable television services will put Canadian cable television companies and other information and service providers in possession of a

great deal of personal information; it needs to be protected not only against abuse by cable companies and other third parties, but also by anyone who succeeds in stealing such personal information. The widespread introduction of electronic mail systems also means that personal information in such communications will lose the traditional protections for confidentiality found in postal legislation, unless new laws are fashioned. Electronic mail in particular creates attractive opportunities for unauthorized access to data for law enforcement purposes, especially when carriers maintain backup tapes on a continuing basis. I would urge attention to the interests of data subjects as well as data owners.

Privacy advocates are customarily urged to show what problems exist before legislators are willing to proceed with the fashioning of remedies. We are most fortunate in having available for such purposes the findings of Mr. Justice Krever's Royal Commission of Inquiry into the Confidentiality of Health Information in Ontario, which is achieving fame for its detailed documentation of abuses of personal privacy through unlawful and unauthorized access to automated and manual health records. This report documented the extraordinary abuses of such data that had been occurring. It demonstrated that despite a general obligation of confidentiality for all employees, operators of the OHIP system gave out data on individuals for law enforcement purposes in violation of the law.⁹ Mr. Justice Krever wrote that "History does not justify blind trust or confidence that confidential health information would be obtained only in situations authorized by the current state of law as it may exist from time to time."¹⁰ The report concluded that the officials running OHIP "did not give confidentiality a high priority. They were primarily concerned with the efficient processing of claims."¹¹ I would submit that this statement characterizes a continuing situation in our society with respect to personal information systems; concern for privacy and security usually loses out to the need for efficiency.

Although I have chosen to highlight the abuse of health information for law enforcement purposes, including RCMP attempts at surveillance of two candidates who had run for Parliament in 1974 on behalf of a lawful political party,¹² the Krever report also includes a general discussion of the threats to privacy presented by the security systems used in computer-supported health systems.¹³ Mr. Justice Krever recognized the extent to which adequate security is essential for the protection of confidentiality; his report includes a list of minimum standards for security, prepared by a consultant, which I recommend to this Committee's attention.¹⁴ The Krever findings are especially relevant to persons seeking evidence of the risks to individual and organizational interests posed by the lack of appropriate computer security.

On the latter point I would like to emphasize what may be well-known to your Subcommittee, namely that existing protections for the security of personal information in computer systems are woefully inadequate. In fact, this is still often the case in North America for non-personal data. Lay people like ourselves assume that appropriate security exists, failing to understand that large computer systems were and continue to be designed to work faster and faster (a process in which security can interfere), to be user friendly, and to be very accessible to users within a government department or a national company. Security incurs costs in both time and money. Thus most large mainframe computers have minimal security protections, as can be demonstrated by the limited number of customers for security systems as compared to the number of such computers in operation. Sometimes high-quality security packages are not even available for non-IBM systems. One is faced with a situation where even if security systems are available, they are not being used. I submit that your Subcommittee should be interested in such matters, not only because of the risks of computer-related crime but also because of the existing challenges to the privacy of persons living and working in this country.

3. Statutory Provisions for the Confidentiality and Security of Personal Information in Privacy and Data Protection Laws

It may be useful to this Subcommittee's consideration of legislation on computer-based crime for me to review existing and proposed provisions in foreign privacy and data protection legislation for the control of unauthorized access to and disclosure of personal information and also for the establishment of security standards. I think it is significant and relevant to your deliberations that the Canadian federal Privacy Act of 1982 does not contain similar measures; the gap could well be filled by the kinds of measures that this Subcommittee may bring forward. The following review covers the relevant measures in national data protection laws, the equivalent of our Privacy Act, in the order in which the statutes were first enacted.

The Swedish Data Act, as amended in 1982, requires the Data Inspection Board to issue regulations to protect privacy in personal information systems in both the public and private sectors, including measures for "control and security." Infringement of such regulations is punishable by a fine or imprisonment for up to one year.¹⁵ Another provision requires the responsible keeper of any file of personal data to ensure their protection against "unlawful alteration or dissemination."¹⁶ A responsible keeper, and anyone else involved in maintaining an information system, "may not without authorization reveal what he has learnt from it concerning the personal circumstances of an individual."¹⁷ Finally the Data Act contains the novel concept of data trespass as a criminal offense: "Any person who unlawfully procures access to a recording for automatic data processing or unlawfully

alters or obliterates or enters such a recording in a file shall be sentenced for data trespass to a fine or to imprisonment not exceeding two years, unless the offence is punishable under the Penal Code."¹⁸

The American Privacy Act of 1974 also contains criminal penalties for matters relevant to the current discussion:

Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000....

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.¹⁹

It is also worth noting that the Privacy Act subjects federal agencies "to civil suit for any damages which occur as a result of wilful or intentional action which violates any individual's rights under this Act."²⁰ Finally, the statute requires federal agencies to establish security standards. Each agency that maintains a system of records shall:

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;²¹

The Federal Republic of Germany enacted its federal data protection act, known as the act on protection against the misuse of personal data in data processing, on January 27, 1977. It punishes anyone disseminating or obtaining "protected confidential personal data" with a fine or a term of imprisonment not exceeding one year. "Where the offender commits his offenses in exchange for payment or with the intention of enriching himself or another person or of harming another person, he shall be liable to a term of imprisonment not exceeding two years, or to a fine."²¹

The French have an expansive national data protection law of January 6, 1978 concerning informatics, data files, and individual freedom. The act mandates the protection of automated personal information in both the public and private sectors: "Any person processing personal data or ordering such processing is required, with respect to the persons

concerned, to take all precautions necessary to protect the security of the information and in particular to prevent it from being distorted, damaged or disclosed to unauthorised third parties."²² Breaches of such requirements are punishable by imprisonment from one to five years, fines from 20,000 to 2,000,000 francs, or both.²³ Moreover:

Any person who, in connection with recording, filing, transmittal or any other form of processing, obtains personal data, disclosure of which would impair reputation or standing or invade privacy, and who knowingly and without the authorisation of the person concerned discloses such data to any party not authorised to receive them under this or any other Act, shall be imprisoned for two to six months, fined 2,000 to 20,000 francs, or both.

Whoever imprudently or negligently discloses or allows disclosures of data described in the preceding paragraph shall be fined 2,000 to 20,000 francs.²⁴

The important French law also permits the National Commission on Informatics and Freedom to "lay down standard rules for systems security as necessary; in exceptional circumstances it may prescribe security measures including the destruction of storage media." The Commission sets forth guidelines for security on July 21, 1981.²⁵

I think that members of this Subcommittee will be particularly interested in certain measures contained in the Data Protection Bill passed by the British House of Lords on March 24, 1983, which is currently before the House of Commons. It has particular importance for other English-speaking countries because it adopts a European system of data protection for both the public and private sectors. The bill establishes the basic principle that "personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."²⁶ The Data Protection Registrar may issue enforcement notices or de-registration notices for non-compliance with this principle.²⁷ Another basic principle of data protection for personal information in the hands of registered data users or computer bureaux is that "appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data...."²⁸ A subsequent clause indicates that in interpreting this principle, "regard shall be had (a) to the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and (b) to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data."²⁹ Furthermore, the U.K. Data Protection Bill includes provisions for punishing breaches of the main part of the act.³⁰ Finally, it prohibits unauthorized disclosure of personal

information by a computer bureau under criminal sanctions and provides for compensation in the form of damages to a data subject who suffers unauthorized disclosure of his or her data.³¹

Two recent international efforts to harmonize national data protection laws are relevant to this statutory survey. On September 23, 1980 the Council of the OECD adopted a recommendation on guidelines governing the protection of privacy and transborder flows of personal data. All member countries have now signed these Guidelines, except Canada, Australia, and Ireland. It is relevant for our present purposes to note that Article 11 of the Guidelines contains a security safeguards principle designed to apply to both the public and private sectors: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."³² The Explanatory Memorandum accompanying the Guidelines notes that although security and privacy issues are not identical, "limitations on data use and disclosure should be reinforced by security safeguards," including physical measures, organizational measures, and informational measures.³³

In January 1981 the Council of Europe opened for signature and ratification its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Almost a dozen European member states have signed the Convention and Sweden has ratified it. The French government is in the process of ratification. Since ratification by the requisite five states is anticipated in 1983, the Convention will soon have the force of law within signatory nations. The Convention includes the need for security as a basic principle of data protection: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."³⁴ Article 10 of the Convention requires parties to "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."³⁵

To bring the discussion to an end closer to home, I would like to draw your attention to similar provisions in the innovative Québec Law 65 of 1982 on access to public documents and the protection of personal information. For data on individuals in the public sector the statute provides that "nominative information is confidential unless the person the information concerns authorizes its disclosures."³⁶ Declarations made to the Commission on Access to Information have to include a description of security measures "taken within the public body to ensure the confidentiality of the nominative information and its use according to the purposes for which it was collected."³⁷ The same Commission "may prescribe

conditions applicable to a personal information file with which the public body must conform and respecting, in particular,...(3) the security measures that must be taken to ensure the confidentiality of nominative information."³⁸ Under the Quebec act the government can also issue regulations "fixing appropriate security standards to ensure the confidentiality of the information entered in a personal information file."³⁹ Finally, there are penal provisions in the act for unlawful disclosure of governmental personal information and general sanctions covering contraventions of the statute.⁴⁰

4. Concluding Observations

1. Proposed federal legislation on computer-related crime should include the protection of personal privacy, since a considerable amount of personal data is stored in automated information systems in both the public and private sectors.

2. Proposed legislation on computer-related crime can be a valuable source of additional protections for privacy in a situation where existing federal, and especially provincial, statutory protections for privacy are largely inadequate. In particular, use of the criminal law to prohibit unauthorized access to, and unauthorized disclosure of, personal information and to establish and enforce security standards will have particular benefits for personal privacy, especially in the private sector, which is generally unregulated with respect to the protection of privacy interests.

3. Canada should follow the example of other Western European nations discussed above in fashioning statutory criminal sanctions regulating unauthorized access to, and disclosure of, personal information and for the creation of mandatory security regimes.

4. There are questions about the ultimate utility and feasibility of using criminal sanctions for the protection of privacy, although there is little doubt in my mind that they would do a useful job of consciousness-raising about the importance of privacy interests, especially among custodians of personal information in the private sector. In fact, since American experience with their Privacy Act indicates that criminal prosecutions under it are rare, one can anticipate a similar scenario unfolding in Canada. I still believe that criminal statutes on computer-based crime should touch on such matters.

Notes

1. David H. Flaherty, Privacy in Colonial New England, University Press of Virginia, Charlottesville, 1972.
2. David H. Flaherty, Privacy and Government Data Banks. An International Perspective, Mansell, London, U.K., 1979.
3. U. S. Department of Justice, Bureau of Justice Statistics, Computer Crime. Legislative Resource Manual (Washington, D.C., 1980), p. 39 and chapter 3.
4. Report of the Commission of Inquiry into the Confidentiality of Health Information (3 vols., Toronto, Ontario, 1980), II, 124. Hereafter cited Krever Report.
5. For a review and listing of the situation with respect to health information in Ontario, see Krever Report, II, 55-63 and III, 368-432. For a review and listing of U.S. federal and state legislation, see Department of Justice, Computer Crime, pp. 40-8 and Appendix E.
6. See U.S. Department of Justice, Computer Crime, p. 40.
7. I am grateful to John D. McCamus of Osgoode Hall Law School for discussing this point with me.
8. An act to enact the Access to Information Act and the Privacy Act, S.C. 1980-81-82, c. 111; An act respecting Access to documents held by public bodies and the Protection of personal information, S.Q., 1982, c. 30.
9. Krever Report, II, 3-7, 23, 62.
10. Ibid., II, 13.
11. Ibid., II, 71.
12. Ibid., II, 11.
13. Ibid., II, ch. 13.
14. Ibid., II, 182-7.
15. Swedish Data Act, 1982, sections 6(10) and 20(2).
16. Ibid., s. 7(4).

17. Ibid., s. 13.
18. Ibid., s. 21.
19. U.S. Privacy Act, 5 USC 552a, s. 2(i)(1) and s. 2(i)(3).
20. Ibid., s. 2(b)(6).
21. Federal Republic of Germany, Federal Data Protection Act of 27 January, 1977, s. 41.
22. France, Act 78-17 of 6 January 1978 on Informatics, Data Files and Individual Freedom, Journal Officiel, January 7, 1978, Article 29. I have generally relied on OECD translations of the European data protection laws, except as in this case, when I have modified a translation myself. Article 29 can also apply to manual files under Article 45.
23. Ibid., Article 42.
24. Ibid., Article 43.
25. Ibid., Article 21(3), and Commission Nationale de L'Informatique et des Libertés, Informatique et Libertés. Textes et documents (Journal Officiel, No. 1473, 6th edition, Feb. 20, 1983, Paris, France), pp. 99-100.
26. Data Protection Bill [H.L.], Schedule I, Part 1, 3.
27. Ibid., clauses 10 and 11.
28. Ibid., Schedule I, Part 1, 8.
29. Ibid., Schedule I, Part 2, 6.
30. Ibid., clause 19(2).
31. Ibid., clause 15(1) to (3) and 23(1).
32. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, Paris, 1981), p. 10, Article 11.
33. Ibid., p. 31.
34. Convention, Article 7, which can be found in U.K. Home Office, Data Protection. The Government's Proposals for Legislation (Cmd. 8539, April, 1982, Her Majesty's Stationery Office, London), p. 11.

35. Convention, Article 10 in ibid., p. 12.
36. An act respecting access to documents held by public bodies and the Protection of personal information, S.Q., 1982, c. 30, s. 53.
37. Ibid., S. 76(5).
38. Ibid., s. 76(3).
39. Ibid., s. 124(5).
40. Ibid., sections 159, 162.

APPENDICE «COMP-1»

Témoignage de David H. Flaherty sur les répercussions de la criminalité informatique sur la protection de la vie privée. Déclaration faite devant le Sous-comité sur les infractions relatives aux ordinateurs du Comité permanent de la justice et des questions juridiques de la Chambre des communes. Ottawa, le 3 mai 1983.

Je m'appelle David H. Flaherty et je suis professeur d'histoire et de droit à la University of Western Ontario de London. Je suis heureux de pouvoir exprimer mon opinion au Comité sur les répercussions que les infractions relatives aux ordinateurs auront sur la protection de la vie privée.

J'aimerais tout d'abord vous dire comment j'en suis venu à m'intéresser au domaine de la protection de la vie privée. J'ai étudié divers aspects de ce domaine depuis que le professeur Alan F. Westin de l'Université Columbia m'a initié à la question en 1964. Mon premier livre portait sur une étude du concept de la vie privée en Amérique, au XVIIe et au XVIIIe siècles.--(1)

Depuis 1974, j'étudie les problèmes contemporains que pose la protection de données en Europe de l'Ouest et en Amérique du Nord. L'ouvrage que j'ai publié en 1979, Privacy and Government Data Banks. An International Perspective, était une étude, menée dans cinq pays, des problèmes que créent la collecte et l'emploi, aux fins de la recherche et de la statistique, de renseignements personnels compilés par les organismes gouvernementaux.--(2)

Je dirige présentement un projet de recherches, de trois ans (1981-1984) qui porte sur une comparaison de la protection des données informatiques, assurée par divers pays de la collectivité mondiale: «Data Protection Compared: An International Perspective.» Essentiellement, j'étudie le mode de fonctionnement des lois sur la protection des renseignements personnels et de la vie privées dans le secteur public (et principalement à l'échelle nationale) aux États-Unis, au Canada, dans la République fédérale d'Allemagne, en France, en Suisse et au Royaume-Uni. Le financement de ce travail de recherche est assuré par la Ford Foundation et par le Conseil de recherches en sciences humaines du Canada. J'ai également récemment terminé, pour le ministère ontarien des Transports et des Communications, une étude des répercussions que peuvent avoir les services de télédistribution bidirectionnels sur la protection de la vie privée.

J'ai reçu votre invitation à comparaître devant le Comité le vendredi 29 avril; ainsi, ce que vous avez devant vous représente en quelque sorte des idées que j'ai mises sur papier au cours d'un weekend; n'oubliez pas que je ne suis en aucune façon, un expert en matière de criminalité informatique. Je ne peux vous offrir que quelques pensées sur les rapports qui existent entre les délits informatiques, la protection de la vie privée et le besoin d'assurer un certain degré de sécurité dans les systèmes informatiques. Plus précisément, j'aimerais attirer votre attention sur les risques d'intrusion de la vie privée que présente l'emploi illégal d'ordinateurs et sur l'opportunité de prévoir des dispositions relatives à la protection de la vie privée dans une loi traitant des délits informatiques.

Je dois avouer ne m'être pas vraiment préoccupé de la protection de la vie privée dans le contexte du débat qui a cours sur la criminalité informatique, et reconnais que cela traduit un manque de perception de ma part. Je suis cependant heureux de dire que l'auteur d'un récent ouvrage de référence sur les délits informatiques, préparé par le Département de la Justice des États-Unis, consacre un de ses quatre chapitres à la sécurité et à la protection de la vie privée, ainsi qu'aux infractions relatives aux ordinateurs.--(3) C'est de cet aspect que je vous parlerai aujourd'hui.

1. La criminalité informatique et la sécurité et la protection de la vie privée

J'aimerais étudier les arguments présentés pour et contre l'opportunité de formuler de nouvelles lois sur la criminalité informatique afin de renforcer les mesures actuelles de protection de la vie privée des particuliers, à la fois dans le secteur privé et dans le secteur public. Bien qu'il soit probablement vrai que l'ensemble des données contenues dans les systèmes informatiques ne touche pas des particuliers facilement identifiables, il n'en demeure pas moins qu'un grand nombre de renseignements personnels est stocké dans les ordinateurs et que leur protection soulève de nombreuses questions rattachées à la protection de la vie privée. Je n'aborderai donc que la question des renseignements stockés dans des systèmes informatisés, dont bon nombre sont assez délicats, comme ceux qui sont stockés dans les systèmes informatisés des secteurs de la médecine, des finances et des banques, des impôts et du droit pénal. L'accès non autorisé à ces renseignements personnels, leur vol ou encore leur divulgation non autorisée posent évidemment des problèmes considérables pour la protection de la vie privée.

On peut soutenir que le droit pénal devrait prévoir pour les citoyens, des mesures visant à protéger leur vie privée et les renseignements personnels compilés à leur endroit. Dans la même veine, des mesures législatives visant à contrôler les délits informatiques devraient également assurer la protection du caractère confidentiel des renseignements personnels stockés dans les systèmes informatiques. Par exemple, le vol de renseignements personnels, pour quelque raison que ce soit, y compris leur acquisition illicite et l'atteinte au droit à la vie privée, pourrait être mieux protégé par une telle mesure législative que cela n'est actuellement le cas. Les intérêts auxquels on nuit dans de telles affaires ne sont pas seulement ceux des propriétaires des données, mais également ceux des personnes sur lesquelles portent ces données. S'il n'en est pas déjà ainsi, l'accès non autorisé à des systèmes contenant des renseignements personnels, comme les banques de données du gouvernement, les dossiers personnels et les dossiers de santé, ainsi que les données de recherches confidentielles, devrait constituer une infraction criminelle.

En plus de l'accès et de la divulgation non autorisés, les mesures législatives visant à contrôler les délits informatiques devraient prévoir des normes et des exigences en matière de sécurité afin de protéger les intérêts des particuliers, particulièrement dans le secteur privé. Une loi à cet effet

ne protégerait pas seulement les intérêts du propriétaire des données contre l'employé indiscret ou méchant, mais également les intérêts privés des personnes sur qui portent ces données informatiques. Comme le juge Krever l'a fait remarquer dans son étude remarquable sur la confidentialité des dossiers de santé, «la vérité est que... le plus grand risque sécuritaire ne découle pas de l'existence du logiciel ou du matériel, mais plutôt des exploitants du système.»--(4)

Il semble évident qu'il existe certaines lacunes dans les lois visant à assurer la protection des renseignements personnels stockés dans les systèmes informatiques, particulièrement en ce qui a trait aux risques associés à un accès non autorisé aux données et à leur emploi illicite. Bon nombre de règlements provinciaux et fédéraux interdisent déjà certains types de divulgation et font même parfois de cette activité un acte criminel.--(5) Cela se produit beaucoup moins souvent dans le cas du secteur privé. Mais les protections actuelles de ce genre, au Canada et aux États-Unis, semblent être aléatoires, assez rares, plutôt récentes et apparemment rarement utilisées lors de poursuites criminelles.--(6) La divulgation non autorisée de renseignements personnels n'est souvent pas même considérée comme une infraction. On doit cependant reconnaître que la conception et la rédaction de lois criminelles visant à réglementer certains aspects de l'atteinte à la vie privée peuvent être plus difficiles que la mise au point de mesures protectrices pour les données ayant une valeur commerciale.--(7)

2. Les systèmes informatisés - Problèmes de respect de la vie privée et de sécurité

Mon collègue Neil Vidmar et moi-même avons récemment dirigé un sondage comportant plus de 200 interviews menées auprès d'un échantillon aléatoire de ménages de London (Ontario) afin de connaître l'attitude des répondants vis-à-vis de la question du respect de la vie privée. Même si les résultats du sondage n'ont pas encore été divulgués par nos clients du gouvernement, je peux quand même dire que dans l'échantillon choisi, on a observé que les répondants se préoccupaient à un point étonnant des questions de protection de la vie privée. Cette constatation corrobore d'ailleurs les quelques rares données d'enquête sur le Canada dont on disposait jusqu'alors. Quatre-vingt-dix pour cent des répondants ont dit considérer la protection de la vie privée comme importante ou très importante. Par comparaison avec six autres questions d'ordre social et économique, ils ont dit que la protection de la vie privée est un peu moins importante que l'inflation, le chômage et la criminalité, mais à peine. Par ailleurs, ils y attachent plus d'importance qu'à la prolifération des armes nucléaires, aux grèves et à l'amélioration des relations entre le Québec et le Canada anglais. Par rapport à six autres sujets relatifs aux droits de la personne et à des questions sociales, la protection de la vie privée est tenue pour prioritaire. En tant que défenseur de la protection de la vie privée, ces résultats m'ont surpris. Je vous en fais part parce qu'il s'agit selon moi d'une preuve manifeste que la population canadienne continue à se soucier de la protection de la vie privée. Votre Comité mérite certes des félicitations pour son rôle dans l'adoption, en 1982, de la Loi sur la protection des renseignements personnels, qui vise le secteur fédéral. Néanmoins, parmi les provinces canadiennes, seul le Québec a

adopté une loi analogue pour la protection des données du secteur public. Quant au secteur privé, il échappe pratiquement à toute réglementation.--(8)

Je me contenterai de vous rappeler qu'il existe actuellement de nombreuses possibilités de vol de renseignements personnels ayant des répercussions sur la vie privée et non couvertes par des règles du genre de celles qui existent contre l'écoute téléphonique par exemple. Avec l'avènement des services de télédistribution bidirectionnels, les sociétés canadiennes de télédistribution et d'autres entreprises d'information et de services entreront en possession d'un vaste volume de données personnelles; celles-ci doivent être protégées non seulement contre les sociétés de télédistribution et d'autres tierces parties, mais également contre quiconque réussirait à obtenir frauduleusement ces renseignements. De plus, comme les systèmes de courrier électronique se répandent, les renseignements personnels contenus dans ces communications perdront la protection traditionnelle qu'offre la législation relative aux postes, à moins que de nouvelles lois ne soient adoptées. Le courrier électronique en particulier est vulnérable: il serait facile et tentant d'avoir accès sans autorisation aux données à des fins d'application de la loi, surtout lorsque les sociétés qui exploitent ces services conservent des bandes de secours en permanence. J'estime qu'il faut veiller à préserver les intérêts des personnes visées par les données, ainsi que ceux des propriétaires des données.

Habituellement, on incite les personnes qui prouvent la protection de la vie privée à montrer quels sont les problèmes qui existent avant que les législateurs n'acceptent d'élaborer des mesures correctives. A cet égard, nous avons la chance de disposer des constatations de la Commission royale d'enquête sur la confidentialité des renseignements médicaux en Ontario, dirigée par le juge Krever. Cette Commission a acquis une certaine notoriété pour les dossiers détaillés qu'elle a rassemblés sur des intrusions dans la vie privée commises par des personnes ayant obtenu illégalement et sans autorisation accès à des dossiers médicaux automatisés et manuels. Le rapport de la Commission témoigne, preuves à l'appui, des abus incroyables qui ont été commis. Ce rapport prouve que malgré l'obligation de confidentialité à laquelle sont tenus tous les employés, des employés du RAMO ont contrevenu à la loi et ont communiqué des données sur des personnes à des forces de l'ordre.--(9) Selon le juge Krever, l'histoire ne justifie pas que l'on ait une confiance aveugle, ni que l'on soit tout à fait certain que des renseignements médicaux ne peuvent être obtenus, à l'occasion, que dans des cas autorisés par la loi.--(10) On conclut dans le rapport que les responsables du RAMO n'accordaient pas une grande priorité aux questions de confidentialité et se préoccupaient surtout du traitement efficace des demandes.--(11) D'après moi, cette déclaration est typique de l'attitude de notre société en ce qui concerne les systèmes de renseignements personnels: les préoccupations en matière de respect de la vie privée et de sécurité passent généralement après les questions d'efficacité.

Bien que j'aie choisi de faire ressortir les divulgations illégales de renseignements médicaux à des fins judiciaires, ce qui comprend notamment des tentatives de la GRC qui surveillait deux candidats qui s'étaient présentés à des élections fédérales en 1974 au nom d'un parti politique licite--(12), le

rapport Krever contient également un exposé général des risques pour la protection de la vie privée que comportent les systèmes de sécurité utilisés dans les systèmes informatisés de renseignements médicaux.--(13) Le juge Krever a reconnu qu'il est essentiel d'adopter des mesures de sécurité adéquates pour protéger la confidentialité des données. Son rapport contient une liste de normes minimales de sécurité dressée par un expert, et que je recommande au Comité de consulter.--(14) Les résultats de l'enquête du juge Krever sont particulièrement intéressants pour toute personne cherchant à prouver les risques qu'entraîne pour les personnes et les organisations l'absence de systèmes de sécurité adéquats.

A ce sujet, je tiens à rappeler quelque chose que votre Sous-comité sait sans doute très bien, c'est-à-dire que les systèmes actuels de protection des renseignements personnels stockés sur ordinateur sont loin d'être suffisants. En fait, en Amérique du Nord, même les données n'ayant pas un caractère personnel sont encore souvent mal protégées. Les non-initiés comme nous supposent qu'il existe des mesures de sécurité appropriées faute de se rendre compte que les grands systèmes informatiques ont été et continuent à être conçus pour permettre d'obtenir toujours plus rapidement les résultats souhaités (rapidité que les questions de sécurité peuvent entraver), pour être faciles à utiliser, et pour être très accessibles aux utilisateurs d'un ministère ou d'une grande société. La sécurité coûte du temps et de l'argent. Par conséquent, la plupart des gros ordinateurs à unité centrale ne sont protégés que par des mesures de sécurité minimales, comme en témoigne le faible nombre de clients qui se procurent des systèmes de sécurité comparativement au nombre global d'exploitants. Parfois, il n'existe même pas de modules de sécurité de haute qualité pour les systèmes autres que IBM. De plus, il arrive que même lorsqu'il existe des systèmes de sécurité, on ne les utilise pas. Je pense que votre Sous-comité devrait s'intéresser à ces questions, non seulement en raison des risques de criminalité informatique, mais également à cause des risques possibles d'intrusion dans la vie privée des personnes qui vivent et travaillent dans ce pays.

3. Dispositions statutaires visant la confidentialité et la sécurité des renseignements personnels dans les lois sur la protection de la vie privée et des renseignements personnels

Comme votre Sous-comité étudie la législation en matière de criminalité informatique, il serait peut-être utile que je passe en revue les diverses dispositions existantes et proposées dans les lois étrangères en matière de protection de la vie privée et des renseignements personnels d'empêcher l'accès non autorisé à des renseignements personnels et leur divulgation, et d'élaborer des normes en matière de sécurité. Je pense qu'il est important que vous sachiez que la Loi sur la protection des renseignements personnels adoptée en 1982 ne contient pas de dispositions analogues; cette lacune pourrait être comblée par des mesures que votre Sous-comité pourrait mettre de l'avant. Le compte rendu qui suit traite des mesures pertinentes énoncées dans les lois étrangères portant sur la protection de l'information; elles sont le pendant de notre Loi sur la protection de la vie privée et sont exposées dans l'ordre dans lequel elles ont été promulguées.

La Data Act suédoise, modifiée en 1982, exige que la Commission d'inspection de l'information établisse des règlements visant à protéger les renseignements personnels contenus dans les systèmes d'information établis dans le secteur public et le secteur privé, et prenne des mesures de «contrôle et de sécurité» à cette fin. Quiconque enfreint le règlement est passible d'une amende ou d'une peine d'emprisonnement d'au plus un an.--(15) Une autre disposition exige que le dépositaire autorisé de tout fichier de renseignements personnels protège ce dernier contre «toute falsification ou divulgation illégale».--(16) Tout dépositaire autorisé et toute autre personne chargée de tenir un système d'information, «ne peuvent révéler sans autorisation les renseignements personnels dont ils ont pris connaissance.»--(17) Enfin, la Data Act renferme la nouvelle notion d'infraction au Code criminel en cas d'accès non autorisé à des renseignements: «Quiconque accède à un enregistrement aux fins de traitement automatique de l'information, ou encore falsifie ou oblitère cet enregistrement ou l'inscrit dans un fichier, sans que la loi ne l'y autorise, est coupable d'accès non autorisé à des renseignements et passible d'une amende ou d'une peine d'emprisonnement d'au plus deux ans, sauf si l'infraction relève du Code criminel.»--(18)

Adoptée en 1974, la Privacy Act des États-Unis prévoit également des peines à l'égard des infractions qui nous occupent actuellement:

Tout agent ou employé d'un organisme qui, de par son emploi ou son poste officiel a en sa possession des dossiers appartenant à cet organisme, ou y a accès, que ces dossiers contiennent des renseignements permettant d'identifier une personne, et dont la divulgation est interdite aux termes du présent article ou d'une règle ou d'un règlement connexe et qui, sachant que la divulgation de ces renseignements précis est interdite, les divulgue à dessein, de quelque façon que ce soit, à toute personne ou à tout organisme n'étant pas autorisé à les obtenir, est coupable d'une infraction et passible d'une amende d'au plus 5 000 \$... (3) Quiconque, sciemment et à dessein, demande à un organisme ou obtient de ce dernier, par des moyens frauduleux, un dossier personnel, est coupable d'une infraction et passible d'une amende d'au plus 5 000 \$.--(19)

Il convient également de noter que la Privacy Act américaine rend les organismes fédéraux possibles «de poursuites civiles à la suite de tout préjudice découlant d'un acte prémédité ou délibéré qui viole les droits de la personne énoncés dans la loi.»--(20) Enfin, la loi exige que les organismes fédéraux établissent des normes de sécurité. Tout organisme qui possède un système de tenue de dossiers doit:

(10) prévoir des méthodes d'ordre administratif, technique et matériel permettant de préserver le caractère confidentiel des dossiers et de les protéger contre toute menace ou tout danger qui pourrait causer à toute personne visée par les renseignements des préjudices, de l'embarras, des inconvénients ou une injustice graves;--(21)

Le 27 janvier 1977, la République fédérale d'Allemagne adoptait une loi sur la protection des renseignements, connue plus précisément comme la loi sur

la protection contre l'usage impropre de renseignements personnels dans le traitement des données. Elle impose à quiconque divulgue ou obtient «des renseignements personnels et confidentiels» une amende ou une peine d'emprisonnement d'au plus un an. «Si le contrevenant commet cette infraction moyennant rétribution, ou dans le dessein de s'enrichir ou d'enrichir un tiers, ou encore de porter préjudice à un tiers, il est passible d'une amende ou d'une peine d'emprisonnement d'au plus deux ans.»--(21)

Depuis le 6 janvier 1978, la France possède une loi étendue portant sur la protection de l'informatique, des fichiers de données et de la liberté individuelle. La loi régit la protection des renseignements personnels automatisés dans le secteur public et le secteur privé: «Quiconque traite des renseignements personnels ou en ordonne le traitement doit, à l'égard des personnes concernées, prendre toutes les précautions nécessaires pour assurer la sécurité de ces renseignements et, plus particulièrement, pour empêcher qu'ils soient déformés, détruits ou divulgués à des tierces parties non autorisées à en prendre connaissance.»--(22) Quiconque enfreint ces dispositions est passible d'une peine d'emprisonnement d'un à cinq ans, d'amendes de 20 000 à 2 millions de francs ou des deux.--(23) En outre,

Quiconque, au moyen d'enregistrement, de classement, de transmission ou de toute autre forme de traitement, obtient des renseignements personnels dont la divulgation pourrait porter atteinte à la réputation de la personne ou constituer une intrusion dans sa vie privée et, sciemment et sans l'autorisation de cette dernière, divulgue ces renseignements à une tierce partie non autorisée à les obtenir aux termes de la présente loi ou de toute autre loi, est passible d'une peine d'emprisonnement de deux à six mois, d'une amende de 2 000 à 20 000 francs, ou des deux.

Quiconque, par imprudence ou négligence, divulgue les renseignements dont il est question au paragraphe précédent ou en permet la divulgation, est passible d'une amende de 2 000 à 20 000 francs.--(24)

Cette importante loi française autorise également la Commission nationale de l'informatique et de la liberté à «établir les règles-étalon nécessaires pour assurer la sécurité des systèmes d'information; dans des cas exceptionnels, elle peut prescrire des mesures de sécurité, y compris la destruction de supports d'information.» La Commission a énoncé des lignes directrices en matière de sécurité le 21 juillet 1981.--(25)

Je pense que les membres du Sous-comité s'intéresseront particulièrement à certaines mesures contenues dans le Data Protection Bill adopté par la Chambre des Lords britannique le 24 mars 1983, et déposé actuellement devant la Chambre des communes. Ce projet de loi revêt une importance particulière pour d'autres pays anglophones, car il prévoit l'adoption d'un système européen de protection des renseignements pour le secteur public et le secteur privé. Le projet de loi établit le principe fondamental selon lequel «les renseignements personnels, quelles que soient les fins pour lesquelles ils sont conservés, ne doivent être utilisés ou divulgués d'aucune façon qui soit

incompatible avec ces fins.»--(26) Le registraire à la protection des renseignements peut émettre des avis de mise en application de la loi ou de déclassification en cas de dérogation à ce principe.--(27) Un autre principe de base inhérent à la protection de renseignements personnels confiés à des usagers de renseignements nominatifs ou à des centres de traitement à façon veut que «des mesures de sécurité appropriées soient prises contre tout accès non autorisé à des renseignements personnels, ou contre la falsification, la divulgation ou la destruction de ces renseignements...»--(28) Un article subséquent indique que, dans l'interprétation de ce principe, «il faut tenir compte a) de la nature des renseignements personnels et des préjudices que pourraient causer cet accès, cette falsification, cette divulgation, cette perte ou cette destruction; et b) de l'endroit où les renseignements personnels sont stockés, des mesures de sécurité programmées dans le matériel pertinent et des mesures prises pour assurer que le personnel ayant accès aux renseignements est digne de confiance.»--(29) En outre, le Data Protection Bill du Royaume-Uni prévoit des peines en cas de violation de la partie principale de la loi.--(30) Enfin, le projet de loi interdit à tout centre de traitement à façon de divulguer sans autorisation des renseignements personnels, sous peine de sanctions pénales, et il prévoit de dédommager quiconque est victime de divulgation non autorisée de renseignements le concernant.--(31)

Deux mesures adoptées récemment au niveau international en vue d'harmoniser les diverses lois nationales sur la protection des données se prêtent bien au présent ouvrage. Le 23 septembre 1980, le Conseil de l'OCDE adoptait une recommandation sur les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Tous les pays membres ont adopté ces Lignes directrices, à l'exception du Canada, de l'Australie et de l'Irlande. Il convient de signaler ici que l'article 11 de ces lignes directrices contient un principe de garantie de la sécurité des données s'appliquant aux secteurs public et privé: «Les données de caractère personnel doivent être protégées grâce à des garanties raisonnables de sécurité contre des risques comme l'accès non autorisé à ces données ou leur perte, leur destruction, leur utilisation, leur modification ou leur divulgation.»--(32) Dans les Notes explicatives accompagnant les Lignes directrices, on note que bien que la sécurité des données et la protection de la vie privée ne soient pas des questions identiques, «les restrictions imposées à l'utilisation et à la divulgation des données doivent être renforcées par des garanties de sécurité», y compris des mesures matérielles, organisationnelles et informationnelles.--(33)

En janvier 1981, le Conseil de l'Europe a tenté de faire signer et ratifier sa Convention pour la protection des particuliers en ce qui a trait au traitement informatique des données de caractère personnel. Presque une douzaine d'États membres de l'Europe ont signé la Convention et la Suède l'a ratifiée. Le gouvernement français s'apprête à faire de même. La condition prévoyant la ratification de document par cinq États devrait être remplie en 1983, si bien que la Convention aura bientôt force de loi au sein des États signataires. Ce document fait état de la nécessité d'adopter des mesures de sécurité un principe de base de la protection des données: «Des mesures adéquates de sécurité doivent être prises pour s'assurer que les données de

caractère personnel emmagasinées dans des dossiers informatiques seront protégées contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé à ces données, ou leur destruction ou leur divulgation illicites.»--(34) L'article 10 de la Convention enjoint aux parties «d'imposer des sanctions et de trouver des remèdes adéquats contre la violation des dispositions des lois nationales donnant effet aux principes de base concernant la protection des données et prévues dans le présent chapitre.»--(35)

Pour ramener la discussion plus près de chez nous, j'aimerais attirer votre attention sur des dispositions semblables contenues dans la loi innovatrice du Québec, la Loi 65 de 1982 sur l'accès aux documents publics et la protection de renseignements personnels. S'agissant des données sur les particuliers dans le secteur public, la loi prévoit que «les renseignements nominatifs sont confidentiels à moins que la personne que ces renseignements concernent n'en autorise la divulgation.»--(36) Entre autres déclarations faites devant la Commission d'étude de l'accès à l'information, il faut signaler une description des mesures de sécurité «prises au sein de l'administration publique pour assurer la confidentialité des renseignements nominatifs et leur utilisation aux fins pour lesquelles ils ont été recueillis.»--(37) La même Commission «peut établir les conditions applicables à un dossier personnel, conditions que doit respecter l'administration publique, tout particulièrement...(3) les mesures de sécurité qui doivent être adoptées pour assurer la confidentialité des renseignements nominatifs.»--(38) Aux termes de la loi québécoise, le gouvernement peut en outre établir des règlements «fixant des normes adéquates de sécurité visant à assurer la confidentialité des renseignements portés à un dossier personnel.»--(39) Enfin, des dispositions pénales sont prévues dans la loi contre la divulgation non autorisée de renseignements gouvernementaux personnels, de même que des sanctions générales pour les personnes contrevenant à la loi.--(40)

4. Conclusions

1. Le projet de loi fédéral sur la criminalité informatique devrait contenir des dispositions sur la protection de la vie privée, beaucoup de données de caractère personnel étant emmagasinées dans des systèmes informatiques à la fois dans le secteur public et le secteur privé.

2. Ce même projet de loi peut s'avérer une source précieuse de protection supplémentaire de la vie privée lorsque les lois fédérales et surtout provinciales sont largement insuffisantes. Tout spécialement, le recours au droit pénal dans le but d'interdire l'accès non autorisé à des renseignements personnels ou la divulgation non autorisée de ces renseignements, ou encore pour établir et appliquer des normes de sécurité, offrira des avantages précis en égard à la protection de la vie privée, surtout dans le secteur privé où, de façon générale, il n'existe pratiquement aucune réglementation en ce domaine.

3. Le Canada devrait suivre l'exemple d'autres pays de l'Europe de l'Ouest discuté plus avant pour définir les sanctions criminelles à prévoir

dans la loi, en ce qui a trait à l'accès non autorisé à des renseignements personnels et à la divulgation de ces renseignements, et créer des garanties de sécurité obligatoires.

4. Certains s'interrogent sur l'utilité et la possibilité d'appliquer des sanctions criminelles pour protéger la vie privée; je suis quasi convaincu qu'elles vont sensibiliser la population à l'importance de la vie privée, surtout chez les protecteurs des renseignements personnels dans le secteur privé. En fait, puisque l'expérience qu'ont acquise les États-Unis avec leur Privacy Act, semble indiquer que peu de poursuites criminelles sont intentées, on peut prévoir que sensiblement la même chose se produira au Canada. Je demeure convaincu que les lois sur la criminalité informatique devraient porter sur ces questions.

Renvois

1. David H. Flaherty, Privacy in Colonial New England University Press of Virginia, Charlottesville, 1972.
2. David H. Flaherty, Privacy and Government Data Banks. An International Perspective, Mansell, London, U.K., 1979.
3. Département de la Justice des États-Unis, Bureau of Justice Statistics, Computer Crime. Legislative Resource Manual (Washington, D.C., 1980), p. 39 et chapitre 3.
4. Rapport de la Commission d'enquête sur la confidentialité des renseignements médicaux en Ontario (3 volumes, Toronto, Ontario, 1980), II, 124. Cité ci-après sous le nom de Rapport Krever.
5. Pour avoir un compte rendu de la situation concernant la confidentialité des renseignements médicaux en Ontario, voir (Rapport Krever, II, 55-63 et III, 368-432. Pour avoir un compte rendu et une liste des lois promulguées par le gouvernement central et les États américains, voir Département de la Justice, Computer Crime, p. 40-48 et Annexe E.
6. Voir Département de la Justice des États-Unis, Computer Crime, p. 40.
7. Je tiens à remercier M. John D. McCamus de la Faculté de droit de Osgoode Hall de s'être entretenu de cette question avec moi.
8. Loi édictant la Loi sur l'accès à l'information et la Loi sur la protection des renseignements, S.C. 1980-1981-1982, c. 111; Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, S.Q., 1982, c. 30.
9. Rapport Krever, II, 3-7, 23, 62.
10. Ibid., II, 13.
11. Ibid., II, 71.
12. Ibid., II, 11.
13. Ibid., II, chapitre 13.
14. Ibid., II, 182-187.
15. Swedish Data Act, 1982, paragraphes 6(10) et 20(2).
16. Ibid., par. 7(4).
17. Ibid., art. 13.

18. Ibid., art. 21
19. U.S. Privacy Act, 5 USC 552a, alinéas 2(i)(1) et 2(i)(3).
20. Ibid., alinéa 2(b)(6).
21. République fédérale d'Allemagne, Federal Data Protection Act of 27 January 1977, art. 41.
22. France, Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel, 7 janvier 1978, article 29. Habituellement, je me reporte aux traductions de l'OCDE pour ce qui est des lois européennes sur la protection des données; toutefois, dans ce cas-ci, j'ai pris la liberté de modifier la traduction. L'article 29 s'applique également aux dossiers manuscrits visés par l'article 45.
23. Ibid., Article 42.
24. Ibid., Article 43.
25. Ibid., paragraphe 21(3) et Commission nationale de l'informatique et des libertés, Informatique et Libertés. Textes et documents (Journal Officiel, no 1473, 6e édition, le 20 février 1983, Paris, France), p. 99-100.
26. Data Protection Bill (H.L.), Annexe I, Partie I, 3.
27. Ibid., Articles 10 et 11.
28. Ibid., Annexe I, Partie 1, 8.
29. Ibid., Annexe I, Partie 2, 6.
30. Ibid., Paragraphe 19(2).
31. Ibid., Paragraphes 15(1) à (3) et 23(1).
32. Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (OCDE, Paris, 1981), p. 10, article 11.
33. Ibid., p. 31
34. Convention, article 7, que l'on peut trouver auprès du U.K. Home Office, Data Protection. The Government's Proposals for Legislation (Cmnd. 8539, April, 1982, Her Majesty's Stationery Office, London), p. 11.
35. Convention, article 10, ibid., p. 12.
36. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, S.Q. 1982, c. 30, art. 53.

37. Ibid., par. 76(5).
38. Ibid., par. 76(3).
39. Ibid., par. 124(5).
40. Ibid., articles 159 et 162.



If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESSES—TÉMOINS

From Western University:

Professor John Palmer, London, Ontario

Professor David H. Flaherty, London, Ontario

De l'Université Western:

Professeur John Palmer, London, Ontario

Professeur David H. Flaherty, London, Ontario

HOUSE OF COMMONS

Issue No. 6

Tuesday, May 10, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 6

Le mardi 10 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

TUESDAY, MAY 10, 1983

(8)

[Text]

The Sub-committee on computer crime met this day at 11:13 o'clock a.m., the acting chairman, Mr. Ken Robinson (*Etobicoke—Lakeshore*), presiding.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From Landspan International of Canada Ltd.: Mr. Peter J. Lawrence, President/Director and Mr. J. Ian Henderson, Vice-president and General Counsel, Ottawa, Ontario.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements and answered questions.

At 12:32 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MARDI 10 MAI 1983

(8)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 11h13, sous la présidence de M. Ken Robinson (*Etobicoke—Lakeshore*), président suppléant.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me}. M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: De «Landspan International of Canada Ltd.»: M. Peter J. Lawrence, président-directeur et M. J. Ian Henderson, vice-président et avocat conseil général, Ottawa, Ontario.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations et répondent aux questions.

A 12h32, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Tuesday, May 10, 1983

• 1112

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): We will call the meeting to order.

We are a little late in getting started, but the bells were ringing and I think we all know what that was all about. We had to be there for the vote. The House adjourned and now it has gone back into session again at 11.00 a.m., so we are a little bit late in getting started.

Our order of reference for this subcommittee is to resume its consideration of the order of reference respecting computer crime. We have before us today two witnesses: Mr. Ian Henderson, the Vice-President of Landspan International of Canada Ltd.; and also Mr. Peter John Lawrence, who is president and director of the same firm.

Which one of you two is going to speak first? Mr. Henderson, you are speaking first, is that it? Fine. Do you have a hand-out or a copy of your remarks which the Chair could have?

Mr. Ian Henderson (Vice-President, Landspan International of Canada Ltd.): Mr. Chairman, we did not bring any prepared remarks, but we do have some information we would like to leave with the subcommittee. We can leave that with you.

First of all, I would like to introduce Peter Lawrence, who is President of Landspan International of Canada Ltd. and is a professional engineer. Because we are dealing with a technical topic, I think it is perhaps best for a professional engineer to talk about the problems at hand.

Mr. Peter John Lawrence (President and Director, Landspan International of Canada Ltd.): Thank you, Mr. Chairman. I would like to confirm our interest in being here and our thanks for the opportunity to give some support to your investigations.

I thought it would be appropriate at this stage of the discussion to maybe define Landspan and our role in the community from a technical point of view. Our company has been a supplier of electronics and telecommunications equipment to the security community within the federal government for the last seven years. We are presently expanding that to create an engineering company within the group to provide a method of developing secure capabilities within Canada that presently are not manufactured, defined or designed here. We would be pleased to discuss that later, if you are interested in that.

• 1115

Our purpose in coming to talk to you is primarily to address the area of technical capabilities in remotely accessing information. When I say "remotely", I mean unconnected remote access, as opposed to having a terminal, which has been

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mardi 10 mai 1983

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À l'ordre, s'il vous plaît.

Nous avons un peu de retard car les cloches sonnaient, nous savons tous pourquoi. Il nous fallait être à la Chambre pour le vote. La Chambre a ajourné puis a ouvert à nouveau la séance à 11 heures. Voilà pourquoi nous sommes en retard.

Le Sous-comité reprend maintenant l'étude de son ordre de renvoi sur les infractions liées aux ordinateurs. Ce matin, nous entendrons deux témoins: M. Ian Henderson, vice-président de *Landspan International of Canada Ltd.*, et M. Peter John Lawrence, président et directeur de la même entreprise.

Lequel de vous doit prendre la parole en premier? Monsieur Henderson? Très bien. Avez-vous plusieurs exemplaires de votre exposé pour la présidence?

M. Ian Henderson (vice-président, *Landspan International of Canada Ltd.*): Monsieur le président, nous n'avons pas de mémoire écrit, mais nous aimerions déposer au Sous-comité un peu de documentation.

Je voudrais d'abord vous présenter Peter Lawrence, président de *Landspan International of Canada Ltd.*, qui est ingénieur de profession. Comme il s'agit d'un sujet très technique, c'est un ingénieur de profession qui est le mieux à même de nous en parler.

M. Peter John Lawrence (président et directeur, *Landspan International of Canada Ltd.*): Merci, monsieur le président. Nous sommes très heureux d'être ici ce matin et nous vous remercions de nous avoir ainsi invités à contribuer à votre étude.

Il serait bon de commencer par vous présenter Landspan et le rôle technique qu'elle joue. Notre compagnie fournit des machines électroniques et de l'équipement de télécommunications aux services de sécurité du gouvernement fédéral depuis sept ans. Nous sommes en train d'ajouter à la compagnie un service de génie qui recherchera une méthode pour mettre au point de l'équipement sécuritaire qui, à l'heure actuelle, n'est ni fabriqué, ni même conçu au Canada. Nous serons heureux d'y revenir plus tard, si cela vous intéresse.

Nous sommes ici ce matin surtout pour vous parler des capacités de la technique à capter à distance de l'information. Quand je dis «à distance», j'entends par là une réception sans connexion, par opposition à une réception avec terminal, ce

[Texte]

referred to a number of times in past testimony—a terminal that would be connected either by telephone or by hard wire. We are talking about unconnected access to information.

We would like maybe to give you an example where if we were talking in this room today with the doors open and we were talking in rather a loud voice, there would be quite a possibility that somebody in the corridor could hear what we were saying. We would not necessarily know that they were listening or that they were interested or uninterested. The fact is we would be transmitting to the point where they could pick it up.

In the same way, most equipment is broadcasting information; most equipment, that is, that has keyboards, video screens, any form of processing information, whether it is an IBM Selectric typewriter, a Wang word processor, an intelligent microprocessor terminal, a computer. What you are able to do in that case is to detect those transmissions. You have a broadcasting capability. There is a recent example where one federal government technical group were measuring the broadcasting of a particular word processing device and they were able to read what was being processed and operated on this terminal nearly three miles away, with no intent of creating a particular investigation of that content, but just to detect the transmission capability of that terminal.

The method of producing this information is that the primary structure of data within these terminals is in a binary or digital format, and therefore it is composed primarily of square waves. These square waves are subject to fast rates of change; even though the amount of voltage is very low, we are looking at what is termed in the industry "spikes" on the leading and trailing edge of these wave forms, and these cause harmonics and sub-harmonics that in effect can be radiated from the equipment.

It would be like comparing an electronic signal at a very high frequency on a piece of wire, which we would call an antenna. When you are getting the very high frequency or high rates of change of levels of these voltages of data within the equipment, you are using any form of spike on a particular length of wire on the circuit boards within the connectors, and it itself will select to use those short lengths of wire as a method of transmitting information, quite accidentally. There is no intent to broadcast; that is just what it does.

The most useful method of protecting against this form of transmission is to screen it. An unclassified word is used, derived from the National Security Agency in the United States, which is termed "tempest", as in the storm tempest. It does not mean anything in itself, but it is an unclassified word that is not in any way a problem in utilizing in and out of the security community. When you talk about a "tempest device", it means that any form of equipment has been secured to a point where it will not radiate the information—the intelligible information.

The purpose of "tempestizing" in a product is to ensure that it will not radiate any compromising emanations; and those are

[Traduction]

dont on a plusieurs fois parlé auparavant, qui pourrait être connectée soit par une ligne téléphonique, soit par un fil. C'est donc un accès à l'information sans aucune connexion.

Par exemple, si nous parlions très fort dans cette pièce-ci et que les portes étaient ouvertes, il serait fort probable que quelqu'un dans le couloir entende ce que nous disons. Nous ne savons pas nécessairement que cette personne écoute, avec intérêt ou non. Nous nous trouverions à transmettre de sorte que l'on puisse nous capter.

De la même façon, la plupart des machines émettent de l'information. Quand je dis la plupart des machines, je parle de celles qui ont un clavier, des écrans cathodiques, de tout ce qui traite de l'information, que ce soit une machine à écrire IBM Selectric, une machine de traitement de textes Wang, un terminal de micro-ordinateur avec intelligence, ou tout simplement un ordinateur. On peut donc dans ce cas capter ces transmissions puisqu'il y a émission. Un exemple récent est fourni par un groupe d'étude technique du gouvernement fédéral qui a mesuré le pouvoir d'émission d'une machine de traitement de textes donnée. On a pu lire l'information traitée sur ce terminal à près de trois milles de là, sans avoir nullement l'intention de décortiquer cette information, mais tout simplement pour savoir quelle était la capacité d'émission du terminal.

Il en est ainsi parce que la structure primaire des données dans ces terminaux est en caractères binaires ou en chiffres qui se composent donc surtout de signaux carrés. Ces signaux carrés varient très rapidement en amplitude comme en fréquence et même pour les microvolts, il se produit ce que nous appelons des «crêtes» au début et à la fin de ces signaux carrés, et ce sont ces crêtes qui créent des harmoniques et des sous-harmoniques qui rayonnent de l'équipement.

On peut comparer cela à un signal électronique d'une fréquence très élevée, passant par un fil que l'on pourrait appeler une antenne. Lorsque les fréquences ou les amplitudes de voltage des données sont très élevées dans l'équipement, vous utilisez n'importe quelle crête sur un segment donné du fil dans les plaquettes qui se trouvent dans les connecteurs. La crête utilise d'elle-même ces courts segments de fil pour transmettre l'information, de façon purement accidentelle. Il n'y a aucune volonté d'émettre; cela se produit tout simplement.

La meilleure protection contre cette forme d'émission, c'est le blindage. On utilise pour cela l'expression non confidentielle «tempest» qui nous vient de l'Agence de sécurité nationale des États-Unis. Ce mot ne veut rien dire en soi, mais on peut l'utiliser sans crainte dans la vie courante puisque ce n'est pas un mot classifié. Quand on parle d'un équipement «tempest», cela signifie que celui-ci est parfaitement protégé contre le rayonnement d'information intelligible.

On blinde ainsi une machine pour s'assurer qu'il n'y aura aucun rayonnement de renseignements secrets. On ne

[Text]

the very effective words which are used in the definition of "tempest". You really do not mind if it radiates when you are switching on and off; that particular interference of radiation does not matter; that is not intelligent.

The methods of protecting against that form of radiation are to build the equipment inside a screen room—and the room could be this size, which is relatively expensive—or you could build a screen completely around the equipment, which could make the equipment relatively heavy and a little difficult to operate; or you could screen it back to the problem area within the equipment. So there are changing philosophies on how technically this can be done, changing because of new methods of protecting and changing also because the levels of voltage and the levels and speed of signals going through the equipment are changing. So there are a number of things that are affecting this whole method of protecting the equipment being built today.

• 1120

I think we are primarily able to discuss here that the broad aspects of the electromagnetic spectrum have to be considered. We have one exhibit, which we will leave with you, from a book on computers and telecommunications, talking about the broad aspects of the electromagnetic spectrum which includes everything from very low frequencies, such as you might hear on a hi-fi set or have on a power line at 50 or 60 cycles, right through to x-rays and gamma and beta rays, which have very high frequencies indeed—you would be into the areas where the frequency is 10 to the power of 23 hertz or cycles per second. We are primarily looking at a very narrow area within that electromagnetic spectrum, termed radio; that would range from 10,000 kilocycles to 10 to the power of 11 cycles or hertz.

Most of the problems we are talking about with regard to equipment broadcasting are within that spectrum, within that radio spectrum. So we are primarily looking at the definition of EMR, electromagnetic radiation, and RFI, radio frequency interference; most of the tempest work to protect it from equipment broadcasting is protected in that frequency range.

One of the questions that would automatically come up in a discussion of this sort is, what are you trying to protect? If the information is in storage—whether it is in a magnetic storage or another form of computer storage, or intelligent processor storage—you are not going to be looking at any radiation because nothing is happening, there is no process taking place. We are primarily addressing the situation whereby the information is being processed, entered into, extracted from, manipulated, or is being transferred by telecommunications wires, hard wire, microwave or whatever, but it is in a process of being changed in some way. That is when there is a vulnerability taking place.

As an example, in one of the minutes of this committee, page 2.13 on March 23, there was a reference there that there was a project Mac, which I think was supposed to be totally secure. The presentation was made to 100 people in an audience, and two military gentlemen in uniform got up, came

[Translation]

s'inquiète pas du rayonnement de la machine lorsqu'elle est mise en marche ou lorsqu'elle est fermée puisque cela n'a aucune répercussion et ne transmet rien d'intelligible.

La meilleure façon donc de se protéger contre ce genre de rayonnement, c'est d'installer l'équipement à l'intérieur d'une pièce blindée qui pourrait être aussi grande que celle-ci, ce qui coûte donc relativement cher. Vous pourriez aussi construire un blindage autour de l'équipement même, ce qui le rend assez lourd et légèrement difficile à faire fonctionner. Vous pourriez également blinder la partie du système qui cause le problème. La technique pour le faire varie parce qu'il arrive toujours de nouveaux modes de protection et aussi parce que les niveaux des voltages et les niveaux et la vitesse des signaux dans l'équipement varient. Plusieurs facteurs influent donc sur les modes de sécurité choisis pour les appareils.

Les généralités touchant le spectre électromagnétique doivent être prises en considération. Nous vous avons fourni un extrait d'un livre traitant des ordinateurs et des télécommunications où il est question des généralités du spectre électromagnétique. On y aborde toutes sortes de choses depuis les fréquences très basses, comme celles d'une chaîne stéréo ou d'un fil électrique de 50 ou 60 cycles, jusqu'aux rayons X et aux rayons gamma et bêta, dont les fréquences sont extrêmement élevées. En effet, on en arrive là à une fréquence de 10 puissances 23 hertz ou cycles par seconde. Nous ne nous intéressons qu'à un champ très restreint du spectre électromagnétique, le champ radio, qui va de 10,000 kilocycles à 10 puissances 11 cycles ou hertz.

Les émissions problèmes de l'équipement dont nous parlons se font presque toujours dans le champ radio. Il faut donc définir d'abord ce qu'est le R.E.M., le rayonnement électromagnétique, et l'I.F., l'interférence radio. La plupart des blindages protègent l'équipement des émissions dans ces fréquences.

Lors d'une telle discussion, la question qui surgit presque toujours automatiquement, c'est la suivante: qu'est-ce que vous cherchez à protéger? Si l'information est emmagasinée sur un ruban magnétique ou sous une autre forme informatique, par exemple dans un micro-ordinateur avec intelligence, vous n'avez pas besoin de vous préoccuper des rayonnements puisqu'il ne se passe rien. Nous nous occupons surtout de l'information qui est en train d'être traitée, que ce soit de la récupération, de l'extraction, de la manipulation, ou un transfert par des lignes de télécommunications, par fils, par micro-ondes ou autrement. Bref, il faut qu'il y ait une opération quelconque. C'est à moment-là que l'information est vulnérable.

Par exemple, à la page 2:13 du compte rendu de la séance du 23 mars, on raconte l'histoire du projet Mac, qui était censé être un ordinateur à toute épreuve. Lorsque l'ordinateur a été présenté à une centaine de personnes, deux militaires en uniforme ont quitté la salle pour y revenir 10 minutes plus tard

[Texte]

back in 10 minutes, and produced the complete list of every password and authorized user of the new totally-secure computer system.

That is not surprising, if this condition of broadcasting were not considered, because although all of the algorithms and protective math entry to get into the computer could be devised, every time these fellows would be sitting operating their equipment somebody could be sitting out here just picking up the information with the proper antenna. So they would be broadcasting—just as if they were sitting in a room shouting and the person who wanted to pick up the passwords were sitting outside the window listening. What the equipment was probably doing was broadcasting. And I am not surprised to see it was uniformed military gentlemen, because that is an area in which it is very difficult to find out what is going on, but very much an area where we in Canada are subject to considerable controls and where there is a considerable interest in this security environment.

One of the areas we have been looking at with regard to protection is in the data transfer area... —electronic data transfer, data processing transfer; within that broad definition we have been attending to the transfer of money, the electronic fund transfer. We have a short article here, out of *The Citizen* about two months ago, in which a broker in a brokerage house in, I think, Rotterdam managed to move \$65 million—but he lost \$2 million. Anyway, the point is that in today's crime, whereby stealing money from a financial institution would take place physically, the robber may have five minutes' headstart on the authorities, because obviously the signals and the alarms would be off. In the process of electronically accessing funds in the process of being transmitted, it might be one or two weeks before somebody could detect what has gone wrong with the checks and balances.

• 1125

In fact, this person disappeared with \$65 million of the private accounts in the Netherlands and abroad, and they have not found him yet, so he had enough head start.

What we are talking about here, of course, is people accessing the funds in transfer. This is not necessarily a broadcasting system, but it is a problem which could require that type of protection. So the previous testimonies that we have understood are primarily addressing the intricacies of writing mathematical programs to protect the access to the information that is being stored. We are primarily trying to address the situation here to you with regard to information being broadcast by accident inadvertently.

Mr. I. Henderson: I think perhaps as a point of explanation you might be interested to know that in the United States there is one company that takes TV ratings, and to take the TV ratings they use an intercept truck and they just drive it through a neighbourhood. As they are going through the neighbourhood, as they pass a house with a television set on they can tell what channel you are watching, because the TV set is emitting a compromising signal. There is an emanation from that TV set, and they can tell precisely what television

[Traduction]

avec en main la liste de tous les mots de passe pour chacun des usagers autorisés de ce nouveau système informatique à l'épreuve de toute intrusion.

Ce n'est pas étonnant quand on ne tient pas compte des possibilités d'émission, car même si l'on peut songer à toutes sortes d'algorithmes et de formules mathématiques pour protéger l'accès à l'ordinateur, chaque fois qu'on fait des opérations avec le système, il peut très bien y avoir quelqu'un tout bonnement assis là en train de capter l'information, s'il a l'antenne appropriée. C'est tout comme s'ils étaient assis dans une pièce en train de crier et que quelqu'un écoutait la conversation assis sous la fenêtre. Le système informatique en cause faisait probablement de l'émission. Je ne suis donc pas du tout étonné de savoir que c'était des militaires en uniforme car c'est un domaine où il est très difficile de savoir ce qui se passe, mais où il y a beaucoup de contrôles au Canada, et auquel les milieux de la sécurité s'intéressent énormément.

Nous avons aussi étudié des façons de protéger le transfert de données électroniques, entre autres le transfert électronique d'argent. Nous avons ici un bref article paru dans le *Citizen* il y a environ deux mois, selon lequel un courtier d'une maison de courtage de Rotterdam a trouvé le moyen de transférer 67 millions de dollars, ou plutôt 65 millions de dollars, car il a perdu deux millions de dollars. De toute façon, de nos jours, ceux qui vont faire des vols dans les succursales d'institutions financières n'ont que cinq minutes d'avance sur les autorités, c'est-à-dire le délai avant que les signaux d'alarme ne se mettent à fonctionner. Pour ce qui est des fonds transmis électroniquement, il peut s'écouler une ou deux semaines avant que quelqu'un détecte la fraude au moment des vérifications.

De fait, cette personne qui a disparu avec 65 millions de dollars tirés de comptes privés au Pays-Bas et à l'étranger court toujours parce qu'elle avait une bonne longueur d'avance.

Il s'agit donc là de personnes qui détournent des fonds en train d'être transférés. Il ne s'agit pas nécessairement d'un système d'émission, mais c'est un problème qui pourrait être réglé par ce genre de protection. Les témoignages antérieurs traitaient surtout des complexités des programmes mathématiques visant à protéger l'accès à l'information emmagasinée. Nous, nous discutons plutôt de l'émission malencontreuse d'informations.

M. I. Henderson: Pour bien vous faire comprendre, j'ajouterais qu'aux États-Unis, il y a une compagnie qui s'occupe des cotes d'écoute pour la télévision qui se sert d'un camion d'interception qui circule tout simplement dans certains quartiers. En passant dans la rue, ce camion peut dire dans quelle maison on regarde la télévision, et même quelle chaîne est syntonisée, car l'appareil de télévision émet un signal identifiable. Le rayonnement de l'appareil permet de dire avec précision quelle chaîne est écoutée. À la fin de la soirée,

[Text]

station you are tuned into. So at the end of the night the computer just prints out a list of what programs you were watching. All electronic equipment, unless it has been tempestized, will give off these electronic signals. So that is just a quick little explanation of precisely what does happen.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Is there any more? Mr. Lawrence.

Mr. P. Lawrence: Quite a bit more, but we would be very pleased to receive questions specifically on any . . .

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): If you have further information that you wanted to give us, because of time restraints it would probably be better for us to get it on the record than to find that we do not have enough questions to get it all.

Mr. P. Lawrence: We have here a list of articles, Mr. Chairman. One is a definition of the electromagnetic spectrum, which will show you the position of the radio frequency within that; an article that was published in *The New York Times* in April this year and reprinted in the *Montreal Gazette* . . .

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Is that a copy of the articles that you have in this file?

Mr. P. Lawrence: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Then maybe we could have these appended to our minutes today. We certainly will not have an opportunity to look at them . . .

Mr. P. Lawrence: No, I would suggest you do that.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): —during this meeting, but we could append them.

Mr. Beatty: We may not want to append them, but certainly we could have them circulated to the members of the committee.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Oh yes, certainly.

Mr. P. Lawrence: Another area that you might look at from the point of view of a reverse problem with regard to the electromagnetic problem we talked about earlier is that during the last few years there has come an awareness that for all of the protection that we might be building there is one threat that we face with regard to the potential explosion of an atomic bomb by the Russians or whomever. By definition, if this bomb were exploded about 50 miles up, say over Kingston, within a radius of 300 miles it would probably blot out everything that we deal with regarding any form of electronics or electrical equipment. You would find 200-amp surges coming up the telephone line in a very short, sharp spurt that would just destroy the circuitry. It would drop out the computer memories that we have. Your car would not work. It would be a total destruction of anything active. It would not

[Translation]

l'ordinateur imprime simplement une liste des émissions qui ont été regardées. Tout équipement électronique, sauf s'il est blindé, émet ces signaux électroniques. Voilà rapidement un exemple de ce qui se passe.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Y a-t-il autre chose? Monsieur Lawrence.

M. P. Lawrence: Il y a des tas d'autres choses encore, mais nous répondrons avec plaisir aux questions précises que vous pourriez avoir.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Si vous avez d'autres renseignements à nous communiquer, il vaut peut-être mieux que vous les donniez tout de suite plutôt que d'attendre les questions car nous n'avons pas beaucoup de temps et il se pourrait bien que nous ne puissions pas poser toutes les questions utiles.

M. P. Lawrence: Nous avons ici une liste d'articles pertinents. L'un porte sur la définition du spectre électromagnétique, qui vous indique le champ des fréquences radio; il y a un article publié dans *The New York Times* en avril dernier et repris par *The Gazette* de Montréal . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Est-ce que ces articles se trouvent dans le dossier que vous nous avez remis?

M. P. Lawrence: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Alors peut-être pourrions-nous les faire annexer au procès-verbal d'aujourd'hui car nous n'aurons certainement pas l'occasion d'y jeter un coup d'oeil . . .

M. P. Lawrence: Je sais, c'est ce que j'allais vous proposer.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): . . . au cours de la réunion d'aujourd'hui, mais nous pourrions les annexer.

M. Beatty: Sans les annexer, nous pourrions en distribuer à tous les membres du Comité.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Certainement.

M. P. Lawrence: Le problème inverse de celui du spectre électromagnétique dont nous venons de parler pourrait vous intéresser. En effet, depuis quelques années, on songe de plus en plus à la protection dont on devrait s'entourer au cas où les Russes ou quelqu'un d'autre feraient sauter une bombe atomique. Par définition, si une telle bombe explosait à 50 milles d'ici, à Kingston par exemple, l'explosion anéantirait tout équipement électronique ou électrique dans un rayon de 300 milles. Il y aurait des pointes très courtes et très rapides de 200 ampères sur les lignes téléphoniques qui détruiraient complètement les circuits. Il y aurait un effondrement de toutes les mémoires des ordinateurs. Votre voiture ne démarrerait plus. Tout ce qui bouge serait une perte totale. Cela ne blesserait pas les êtres humains, mais ce serait superflu puisque de toute façon ils deviendraient complètement inefficaces.

[Texte]

hurt any human beings, but you would not need to hurt them because they would be totally ineffective. This is referred to as EMP, electromagnetic pulse, and there is a serious concern by the security community that equipment has to be—the reference is “hardened” against this type of attack.

The equipment that we talked about earlier that might be protected from radiating or broadcasting information would have to be completely screened. The same screening process will provide a reverse protection from electromagnetic pulse interference. That is just an aside to you.

In that list of exhibits there you will find that there are some articles and also brochures on particular equipment that we are very familiar with regarding word processing, text editing, digital voice equipment, electronic fund transfer protection—and I think you might find those interesting to expand on some of these.

Mr. I. Henderson: And encryption.

Mr. P. Lawrence: Mr. Henderson just referred to encryption. Although the encryption is an important aspect, it is the method of coding that information when you are transmitting it so that nobody can necessarily decode it. Each one of these subjects could get very deep and fairly lengthy, so we are trying to skip through and to give a broad picture of the situation. If there is any discussion on any of these we would be pleased to follow along.

• 1130

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Beatty, do you wish to start off with the questioning?

Mr. Beatty: Thank you, Mr. Chairman.

First of all, let me thank Mr. Henderson and Mr. Lawrence for a very useful presentation. Although the scope of your presentation is somewhat broader than the project before us dealing with legislation on computer crime, I think an understanding of the technological capabilities is something essential if we are to succeed in the project.

The issue of electromagnetic pulse has been an area of interest to me now for about a year or so; I have been trying to get some information from our government, as well as from other sources, as to what sort of work is being done here. One of the things I have found shocking is that virtually no work has been done by the Government of Canada in this area, and no attempt made at all, to the best of my knowledge, to harden federal systems against EMP. There seems to be the assumption that it is just one of those things that, should it happen, we will deal with it at that time; but it might be a little too late then. However, I guess we will have to set that aside for today's purposes in that it goes well beyond the scope of the project itself.

My curiosity was very much piqued though by the illustration you gave of a word processing machine where one was able to decode what was being put into the machine three

[Traduction]

C'est ce qu'on appelle la P.E.M., la pulsation électromagnétique, et les services de sécurité croient vraiment que l'équipement devrait être protégé contre ce genre d'explosion.

L'équipement dont on a dit plus tôt qu'il devait être protégé du rayonnement ou de l'émission d'information devrait être complètement blindé. Ce même blindage assurerait une protection inverse contre l'interférence de pulsations électromagnétiques. Je vous dis cela en aparté.

Dans cette documentation, vous trouverez des articles et des brochures sur l'équipement que nous connaissons bien, à savoir les machines de traitement de textes et de mots, les micronumériques, le système de protection pour les transferts électroniques d'argent, et vous voudrez probablement vous attarder à certains.

M. I. Henderson: On parle aussi de chiffrement.

M. P. Lawrence: M. Henderson vient de parler de chiffrement. Même si cette méthode est importante, c'est tout simplement une façon de coder l'information transmise afin que n'importe qui ne puisse pas la décoder. Chacun de ces sujets, à lui seul, pourrait prendre beaucoup de temps, et nous avons donc essayé de vous donner une idée d'ensemble de la situation. Maintenant, si vous voulez que nous approfondissions certains sujets, nous le ferons avec plaisir.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Beatty, vous voulez commencer?

M. Beatty: Merci, monsieur le président.

Pour commencer, je veux remercier MM. Henderson et Lawrence pour cet excellent exposé. Je sais bien que vous avez dépassé le cadre de notre sujet proprement dit, puisque nous sommes ici pour discuter de la législation sur les infractions liées aux ordinateurs, mais si nous voulons réussir dans notre entreprise, nous devons également comprendre les aspects technologiques du problème.

Le problème des pulsions électromagnétiques m'intéresse maintenant depuis près d'un an. J'ai essayé de trouver des informations à ce sujet auprès de notre gouvernement et également en m'adressant à d'autres sources; j'ai cherché à savoir ce qui se faisait. Une chose m'a frappé, le fait que le gouvernement du Canada n'ait pratiquement rien fait dans ce domaine, aucune tentative, que je sache, pour rendre les systèmes fédéraux moins vulnérables à ce type de criminalité. On semble attendre d'être placé devant le fait accompli pour faire quelque chose. Malheureusement, cela risque d'être trop tard. Toutefois, je n'approfondirai pas plus cet aspect de la question aujourd'hui car il dépasse quelque peu notre sujet.

Vous avez cité l'exemple d'une machine de traitement de mots dont on avait pu décoder les opérations à trois milles de distance; cela a beaucoup piqué ma curiosité. S'agissait-il d'une machine du gouvernement fédéral?

[Text]

miles away. This was a Canadian federal government word processing machine?

Mr. P. Lawrence: No, it was a Canadian federal government study of a commercial word processing device.

Mr. Beatty: Not owned by the federal government, but similar?

Mr. P. Lawrence: Probably rented by. It is a very well-known company, which I will not mention; but it is a standard product that you could buy from a company here in Canada.

Mr. Beatty: Maybe one way of heightening the concern of members of Parliament would be if our Micom's that we have in our offices were emitting . . .

Mr. P. Lawrence: They are.

Mr. Beatty: They are?

Mr. P. Lawrence: Yes. But Micom is also a company that is paying attention to this tempest requirement. Although they have not completed it yet, it is a very difficult thing to achieve. It is a very strict, and a very closed, community. In fact, finding out what you would have to do to make it tempest is difficult because of the need for a person to know.

Mr. Beatty: When Jim Finch and Colin Rous were here, I showed them the word processing equipment we had in our offices. There is an intention in the House of Commons to set up a local area network, which would enable our word processors to become communicating. I have been intending to follow up with the House administration, because one of the things they pointed out is that, usually with local area networks, when one sends a message from one machine to another, in fact it goes to every machine, but only some machines accept the message. The argument they made was that it is very easy to modify a machine so that it could simply store and forward any message, whether it was intended for it or not. But what you are saying is that with word processing equipment it would be possible, even without any hardware connection to the system, at least to monitor what was taking place in the machine.

Mr. P. Lawrence: That is right, even though you do not particularly want to set up your own personal local area network to communicate by radio between each other with antennas up. But, yes, it would be a compromising problem.

Mr. I. Henderson: It does not matter whether it is an Apple or a Micom if there is an intercept truck sitting outside there listening to what is going on in that word processor or that computer.

Mr. Beatty: Is the problem fundamentally different from the problem of telephones? Surely phone lines pick up . . . my understanding is that in tapping a phone line, you do not necessarily have to put a physical tap on it; that in fact you do get electromagnetic waves emitted that one could . . .

Mr. P. Lawrence: You could have an induction process cut into the phone; yes.

[Translation]

M. P. Lawrence: Non, mais c'était dans le cadre d'une étude sur un appareil de traitement de mots effectuée par le gouvernement fédéral canadien.

M. Beatty: La machine n'appartenait pas au gouvernement fédéral mais était comparable?

M. P. Lawrence: Elle avait dû être louée. C'est une compagnie bien connue que je ne citerai pas, c'est un appareil très courant qu'il est possible d'acheter ici au Canada.

M. Beatty: J'imagine que les députés auraient tout lieu de s'inquiéter s'il était possible d'émettre à partir des appareils Micom que nous avons dans nos bureaux . . .

M. P. Lawrence: Mais c'est possible.

M. Beatty: Oui?

M. P. Lawrence: Oui. Mais d'un autre côté, Micom s'intéresse également à ces dispositifs de blindage. Nous avons là une communauté très fermée, très sévère. En fait, il est déjà difficile de déterminer ce que vous devriez faire pour blinder votre système à cause du besoin de chaque personne de savoir.

M. Beatty: Quand Jim Finch et Colin Rous étaient là, je leur ai montré les appareils de traitement de mots que nous avons dans nos bureaux. La Chambre des communes a en effet l'intention de mettre sur pied un réseau local qui permettrait de faire communiquer chacun de nos appareils. J'avais l'intention de suivre cette affaire avec l'administration de la Chambre car on nous a signalé, entre autres choses, que les réseaux locaux étaient en général disposés de telle sorte que lorsqu'on envoyait un message d'une machine à une autre, toutes les machines du réseau recevaient le message, mais toutes ne l'acceptaient pas. On nous avait fait observer qu'il était très facile de modifier une machine pour qu'elle entrepose et expédie n'importe quel message, qu'il lui soit destiné ou pas. Ce que vous nous dites, c'est qu'un appareil de traitement de mots, même sans aucune modification matérielle du système, pourrait permettre de surveiller les transactions de la machine.

M. P. Lawrence: Exactement. Même sans un réseau local personnel permettant de communiquer par radio avec des antennes. Mais effectivement, le problème serait particulièrement difficile.

M. I. Henderson: Peu importe qu'il s'agisse d'un appareil Apple ou Micom, s'il y a un camion d'interception à l'extérieur de l'immeuble qui écoute ce qui se passe dans cet appareil ou dans cet ordinateur.

M. Beatty: Est-ce que le problème est très différent du problème posé par les téléphones? J'imagine que les écoutes de lignes téléphoniques . . . je crois comprendre que pour écouter les conversations téléphoniques sur une ligne, il n'est pas nécessaire de faire un véritable branchement, il suffit en réalité de capter les ondes électromagnétiques émises . . .

M. P. Lawrence: Effectivement, il est possible de profiter du phénomène d'induction.

[Texte]

Mr. Beatty: So it is not necessary actually to tap the line as such.

Mr. I. Henderson: No, but then when you look at the microwave, many of the long distance calls will be going out over microwaves; so now you are getting into another area where, perhaps, unfriendly nations even in Canada are listening in on long distance telecommunications that are going out over microwave.

Mr. Beatty: Yes. I was just about to get to that. There is a book that was recently written about the NSA and the activities it undertakes to monitor phone messages in the U.S. and around the world for national security.

Mr. P. Lawrence: Foster Palace?

Mr. Beatty: Yes. In addition, there was quite a controversy a few years ago about equipment on the roof of the Soviet embassy in Washington, and I believe also on the Soviet consulate in San Francisco. I believe there is also similar equipment on the Soviet embassy in Ottawa here . . .

Mr. I. Henderson: Yes.

Mr. Beatty: —which enables the monitoring of telephone conversations. Can you explain to the committee something which, although again it goes beyond the issue of computer crime, is very much relevant to it?

• 1135

From talking to people in Bell some years ago when I first raised the issue, my understanding is that our security people monitor the purchase of land by agents or representatives of potentially unfriendly foreign countries. If, for example, they were intending to purchase land near microwave towers for the long-haul network for Bell, this would not be permitted by our government.

I gather from what you are saying that proximity does not happen to be that important, that in fact it can be some distance away and still intercept microwaves.

Mr. P. Lawrence: It depends. In a microwave system you are primarily looking at a purposeful transmission in a particular direction. The reason for having this dish, the thing that looks like a saucer on its side, is that you are concentrating the beam of the transmission. Otherwise, it would just radiate in a normal position area. You would, therefore, have to be in that line of path of the transmission on a microwave system, and so proximity might be very important. Your word processor has no particular direction; it is just radiating.

Mr. Beatty: In the U.S., there is quite a controversy at the present time about the sale of microwave antennas for the unauthorized reception of pay-TV. I guess there have been successful prosecutions, under American legislation, of people who have bought microwave antennas. But here you are not talking about a point-to-point type of beam. You are talking about one that disseminates very broadly.

[Traduction]

M. Beatty: Autrement dit, il n'est même pas nécessaire de faire un véritable branchement.

M. I. Henderson: Non, mais prenez l'exemple des micro-ondes; beaucoup de communications téléphoniques de longue distance passent sur des micro-ondes. Autrement dit, on entre ici dans un domaine tout à fait différent et l'on peut même concevoir que des nations hostiles écoutent les communications sur longue distance qui passent sur les micro-ondes à l'intérieur du Canada.

M. Beatty: Oui. Justement, j'y venais. Un livre vient d'être publié sur la sécurité nationale et les moyens de surveiller les messages téléphoniques aux États-Unis et dans le monde entier à des fins de sécurité nationale.

M. P. Lawrence: Foster Palace?

M. Beatty: Oui. De plus, il y a quelques années il y a eu toute une controverse au sujet du matériel installé sur le toit de l'ambassade soviétique de Washington et également, je crois, du consulat soviétique à San Francisco. Apparemment, il y aurait le même genre de matériel sur le toit de l'ambassade soviétique ici même à Ottawa . . .

M. I. Henderson: Oui.

M. Beatty: . . . qui permet de suivre les conversations téléphoniques. Pouvez-vous nous expliquer une chose qui, bien que n'étant pas liée directement aux crimes d'ordinateurs, lui est tout de même apparentée?

D'après ce que m'en ont dit les gens de Bell il y a quelques années quand j'ai commencé à m'intéresser à la question, apparemment nos responsables de la sécurité surveillent l'achat de terrains par des agents ou représentants de pays étrangers qui pourraient être hostiles. Par exemple, si l'on s'aperçoit qu'ils ont l'intention d'acheter des terres à proximité des antennes micro-ondes du réseau longue distance de Bell, notre gouvernement interdit la transaction.

D'après ce que vous dites, la proximité n'aurait pas une tellement grande importance puisqu'on peut intercepter les micro-ondes à une certaine distance.

M. P. Lawrence: Cela dépend. Dans un système à micro-ondes, les transmissions à certaines fins se font avant tout dans une direction donnée. La raison d'être de cette soucoupe, cette chose qui ressemble à une assiette inclinée, c'est qu'elle permet de concentrer le rayon de la transmission. Autrement, la radiation se fera en position normale et il faudrait donc se trouver sur le chemin de transmission d'un système à micro-ondes: dans ce cas-là, la proximité serait très importante. Votre appareil de traitement de mots n'a pas de direction particulière, il émet de simples radiations.

M. Beatty: Aux États-Unis, il y a actuellement une controverse active sur la vente d'antennes à micro-ondes pour la réception non autorisée de programmes de la télévision payante. Des poursuites judiciaires contre des gens qui avaient acheté des antennes à micro-ondes ont d'ailleurs été couronnées de succès. Mais ici, vous ne parlez pas d'un rayon de type directionnel; il s'agit d'une diffusion très disséminée.

[Text]

I gather the problem is that much more serious when you get into satellite communications, because a satellite beam covers a much broader area. If you were to intercept telephone messages that were being sent by satellite, you would not have to be particularly picky about where you put your antenna. Is that correct?

Mr. P. Lawrence: Right.

Mr. Beatty: Because their footprint is very broad.

Mr. P. Lawrence: Right.

Mr. Beatty: I recently sent to other members of the committee an article from the magazine *Omni*. That article dealt in part with the use of computers to weed through the volume of calls that were going through. I gather one of the biggest problems in dealing with this is not getting into the system, but rather separating the wheat from the chaff, and deciding which messages you want to intercept and which ones you do not. I gather, from the magazine, if it is correct—and perhaps you could confirm it—that the price of technology is coming down very quickly, and that with relatively inexpensive equipment it would be possible to computerize a sorting system that could pick out key words, for example, or could put an intercept on certain telephone exchanges and just tape the messages going to a particular telephone line. Is that correct?

Mr. P. Lawrence: Yes.

Mr. Beatty: It says that this is particularly cost-effective as you get into digital messages because of the encoding that is necessary—I suppose particularly packet-switching equipment, where you would put an address on each packet. Consequently, the computers can sort it out and decide which messages they should be taking much more readily than they would with analog equipment. Is that correct?

Mr. P. Lawrence: Packet-switching... It sounds to me as if there were a slight difference of definition there. In packet-switching you are breaking the single message into a number of packets, and making them into discrete-length components, which can be transmitted separately over different transmission routes and transmission lines and re-assembled at the other end. That gives you a bit of a problem, trying to track down the complete message, if you do not happen to be gathering 90% of that message information. The packets do not all go down the same transmission route.

Mr. Beatty: So you would have to hit one of the bottlenecks in the system where it is re-assembled.

Mr. P. Lawrence: And nobody has caught it.

Mr. Beatty: Then packet-switching itself could provide some security from unauthorized interception.

Mr. P. Lawrence: It does, in effect, yes. In fact that is one international method that is being attempted by, I think, a group in South Africa, who exposed it at a telecommunications conference in Switzerland recently. In this system they were frequency-hopping; they were breaking the transmission into different carriers and just sequentially going through a large

[Translation]

J'imagine qu'avec les communications par satellite, le problème s'aggrave encore parce que le rayon d'un satellite couvre un secteur encore plus étendu. Si vous interceptiez des messages téléphoniques transmis par satellite, vous n'auriez pas besoin de choisir un endroit très précis pour ériger votre antenne, c'est bien ça?

M. P. Lawrence: Absolument.

M. Beatty: Parce que l'empreinte est très étendue.

M. P. Lawrence: Précisément.

M. Beatty: Il y a quelque temps, j'ai envoyé aux autres membres du Comité un article—du magazine *Omni*. On y parlait entre autres choses, de la possibilité de se servir d'ordinateurs pour trier une masse d'appels. Apparemment, un des plus gros problèmes n'est pas de pénétrer dans le système, mais plutôt de trier ce qui est bon de ce qui est inutile, de décider quels sont les messages à intercepter et quels sont ceux qu'il faut rejeter. D'après ce magazine, si l'article est exact, et vous pourrez peut-être me le confirmer—le prix de la technologie est en train de baisser très rapidement et avec un matériel relativement peu coûteux, il va devenir possible de trier les communications par ordinateur pour ne retenir que certains mots clés, par exemple, ou, dans le cas de certains standards téléphoniques, de ne retenir que les messages destinés à un numéro particulier. C'est bien ça?

M. P. Lawrence: Oui.

M. Beatty: De plus, cela serait particulièrement efficace avec les messages digitaux à cause du codage nécessaire surtout dans le cas des blocs de transmission qui sont adressés individuellement. Autrement dit, les ordinateurs peuvent faire le tri et décider quels sont les messages à retenir, et cela, beaucoup plus rapidement qu'avec un matériel analogue. C'est bien ça?

M. P. Lawrence: Les transmissions par blocs... je pense que nous avons un petit problème de définition. Dans les transmissions par blocs, il s'agit d'un message unique qui est ensuite séparé en plusieurs transmissions, c'est-à-dire en composantes de longueurs variées qui peuvent être transmises séparément sur différents canaux de transmission, sur différentes lignes de transmission puis, regroupées à destination. Il devient donc plus difficile d'avoir l'ensemble du message puisque toutes les transmissions ne passent pas par le même itinéraire, il faut reconstituer le message intégral et ce n'est pas aussi facile.

M. Beatty: Autrement dit, il faudrait retrouver un des points de rassemblement du système où le message est réassemblé.

M. P. Lawrence: Et personne ne l'a retrouvé.

M. Beatty: Par conséquent, les messages par envois multiples pourraient offrir une certaine protection contre les interceptions non autorisées.

M. P. Lawrence: Effectivement, oui. D'ailleurs, c'est une des méthodes internationales mises à l'essai par un groupe d'Afrique du Sud qui en a parlé lors d'une conférence récente sur les télécommunications en Suisse. C'était un système qui permettait de sauter d'une fréquence à l'autre et de répartir une transmission sur différents vecteurs; il était possible de

[Texte]

number of carriers, so that anybody trying to trap that particular transmission would have great problems with just tracking where it was in the frequency range.

• 1140

Mr. Beatty: I suppose what the committee has to do, and it is one of the problems that is facing us, is to sort out, when you are dealing with the protection of computerized information, to what extent that protection has to be technological and to what extent it can be legislated. You did not deal with the legislative aspects...

Mr. P. Lawrence: Right.

Mr. Beatty: —in your presentation, which I can understand. But I want to ask you, from a technological point of view, is there such a thing as a truly secure system, or is it simply a matter that you make it sufficiently costly for a potential computer criminal, if you like, to get in, that you believe you price it out of his range?

Mr. P. Lawrence: That, I think, is probably the best way to look at it. It is in relation to cost and time. If a minister is negotiating in a hostage-taking in a penitentiary in British Columbia, then what he probably needs is maybe a security communications system that would give him three or four days before anybody could break it down to find out what his conversation was, by which time the hostage-taking is finished. What he does not want is his conversation in the newspaper the next morning. But that may be a requirement of two, four, six days of protection.

If you are into something at a national security level, you may want it protected for five years, so you have to build a much more expensive, much more complex method of protection. So in actual fact, your complexity of protection is related to the amount of time you are looking for. I think if you are talking about perfect security, you are talking about infinite time, which I think is a relatively difficult thing to talk about.

Mr. Beatty: One can draw an analogy, I suppose, to physical security surrounding a bank. There is no such thing, whether it is Fort Knox or any other institution, as a 100%-secure institution. What you are talking about is making it sufficiently secure that it would discourage people from breaking in.

Mr. P. Lawrence: That is right.

Mr. Beatty: The cost would be too great and likely the protection would be too...

Mr. P. Lawrence: Exactly.

Mr. I. Henderson: In crypto-work you are talking about key depth and how long it is going to take to break the code. Some codes will go for hundreds of years before you are repeating a code. When you have 10 to the 81 times codes that are keyable into a DES unit, then it gives a long time before anybody is going to be able to break that down.

[Traduction]

passer en revue systématiquement toute une série de transporteurs et quiconque aurait essayé de capter cette transmission aurait eu beaucoup de mal à retrouver la gamme de fréquence.

M. Beatty: Vous savez qu'une des tâches de ce Comité sera de déterminer dans quelle mesure la protection des données informatiques devra être de nature technologique et dans quelle mesure il faudra légiférer. Vous n'avez pas traité des aspects législatifs...

M. P. Lawrence: C'est exact.

M. Beatty: ... dans votre exposé, ce que je comprends fort bien. Toutefois, je veux vous poser une question qui relève de l'aspect technologique: est-ce qu'il existe un système véritablement sûr, ou bien la seule solution est-elle de rendre les choses trop coûteuses pour décourager les futurs criminels?

M. P. Lawrence: Je pense que c'est probablement la meilleure façon d'envisager la solution. Il faut axer nos efforts sur le coût et sur le temps. Prenez l'exemple d'un ministre qui négocie avec des preneurs d'otage dans un pénitencier de Colombie-Britannique: il aura besoin d'un système de communication qui reste sûr pendant trois ou quatre jours, autrement dit, il faut que sa conversation reste secrète pendant au moins trois ou quatre jours, c'est-à-dire jusqu'à la fin de l'incident. Ce qu'il veut éviter à tout prix, c'est que cette conversation paraisse dans le journal le lendemain matin. Autrement dit, une protection de deux, quatre ou six jours.

Maintenant, si vous passez au domaine de la sécurité nationale, la protection dont vous avez besoin doit durer cinq ans et par conséquent, la méthode de protection sera d'autant plus coûteuse et d'autant plus complexe. En fait, la complexité de la protection est directement proportionnelle au temps que vous achetez. Si l'on pouvait parler de sécurité parfaite, il s'agirait d'un temps illimité, une notion relativement difficile.

M. Beatty: J'imagine que l'on peut comparer cela aux mesures matérielles de protection d'une banque. Qu'il s'agisse de Fort Knox ou d'une institution quelconque, une protection absolue à 100 p. 100 n'existe pas. Dans tous les cas, il s'agit de décourager les gens par la nature des obstacles.

M. P. Lawrence: Exactement.

M. Beatty: Les coûts seraient trop élevés et la protection serait trop...

M. P. Lawrence: Exactement.

M. I. Henderson: En cryptographie, on a une profondeur—clé et l'inconnue, c'est le temps qu'il faudra pour déchiffrer le code. Il y a des codes que personne ne reproduit pendant des centaines d'années. Quand 10 des 81 éléments du code seulement peuvent être entrés dans un système, il faut vraiment très longtemps avant que quiconque puisse réussir à déchiffrer.

[Text]

Mr. P. Lawrence: Without a lot of expensive computer equipment to attempt to analyze all the permutations and combinations.

Mr. Beatty: Is it not the case that the cost is falling dramatically and that the capabilities of computerized equipment are increasing virtually exponentially year over year?

Mr. P. Lawrence: But, you see, the cost is falling. The capabilities are exponentially increasing, so the capability of creating a complex protection is going up proportionately and therefore the attempt to break it is unfortunately increasing too.

Mr. Beatty: So what you are saying, too, is that security is very much a moving target, that a system that is secure today is not secure tomorrow, and that from the point of view of business or of government-run institutions, it is not good enough to draw up security standards which meet the best of today's standards because tomorrow they are obsolete, and that one must be constantly upgrading the system, unlike perhaps physical security, where it is pretty much predictable what sort of physical threats there might be to an institution 10 years down the line?

Mr. P. Lawrence: If you want to pursue that position of cost and complexity, the fact that the chip—to use a buzz word—has produced a very low-cost method of complex manipulation of information, has resulted in the creation of what Ian has just referred to, the DES, which is the data encryption standard in the United States. The data encryption standard has been involved with the National Security Association, NSA, which...

Mr. Beatty: The National Security Agency, I believe.

Mr. P. Lawrence: Agency—I beg your pardon—which has provided commercial levels of encryption that would be totally confounding to what the high levels of crypto in math and engineering in World War II thought they had. The technological advance that has been made since then has created such an incredible complexity in this form of encryption that now our commercial encryption processes just far exceed anything known in those days, to the point now that we have low-cost, highly available, encryption processes through the complexity of the micro-chip, the silicon chip, which has totally condensed the size of the operating equipment. Of course that involves, in direct proportion, the encryption devices; the key generators, as they are referred to, at national security level, in complexity have also improved.

• 1145

Mr. Beatty: One other technical question: In getting back to the unplanned radiation of electromagnetic waves from equipment, would I be correct in assuming that with the complexity of new electronic equipment, which requires decreasing amounts of power because of the sophistication of the chips used, that in fact the amount then of energy being radiated is reduced at the same time?

[Translation]

M. P. Lawrence: C'est-à-dire sans un matériel d'informatique très coûteux pour analyser toutes les permutations et combinaisons possibles.

M. Beatty: Mais justement, est-ce que les coûts ne sont pas en train de baisser très rapidement, est-ce que les capacités de l'informatique ne se multiplient pas de façon exponentielle d'une année sur l'autre?

M. P. Lawrence: Mais vous voyez, effectivement, les coûts diminuent, les capacités augmentent à un rythme exponentiel mais parallèlement, il devient possible de rendre les mesures de protection encore plus complexes, elles se compliquent proportionnellement.

M. Beatty: Autrement dit, la sécurité est véritablement un cible mouvante, un système sûr aujourd'hui ne le sera pas demain et, pour l'entreprise privée et pour le gouvernement, il ne suffit pas de mettre au point des normes de sécurité conformes aux exigences les plus sévères que l'on puisse avoir aujourd'hui, parce que demain, ce sera dépassé. Bref, le système doit être modernisé en permanence contrairement aux mesures de sécurité matérielles qui sont sous des menaces plus ou moins prévisibles même 10 ans d'avance?

M. P. Lawrence: Si vous voulez des détails à propos du coût et de la complexité, le fait que la puce—pour utiliser un mot du jargon—constitue une méthode très peu coûteuse pour faire des manipulations complexes de l'information a amené la création aux États-Unis d'un système dont Ian vient de parler, le DES, un système de normalisation du chiffage des données. La norme de chiffage des données a été mise au point en collaboration avec *The National Security Association*, NSA, qui...

M. Beatty: C'est la *National Security Agency*, je crois.

M. P. Lawrence: *Agency*. Excusez-moi. Bref, ils ont mis au point des codes commerciaux qui seraient une véritable énigme pour les plus grands spécialistes de cryptographie mathématique et de génie de la Seconde Guerre mondiale. Les progrès technologiques réalisés depuis lors ont permis une complexité incroyable de cette forme de codage et aujourd'hui, nos processus de codage commerciaux sont bien supérieurs à tout ce que l'on connaissait à cette époque. À tel point que les processus de codage actuels sont peu coûteux, très disponibles, grâce à la complexité des micropuces, des puces de silicone, qui ont permis de réduire considérablement la taille du matériel. Évidemment, cela comprend dans une proportion directe, les appareils de chiffement. On les appelle des générateurs de clés, ils servent à la sécurité nationale et sont devenus également beaucoup plus complexes.

M. Beatty: Une autre question d'ordre technique: pour revenir aux radiations non voulues des ondes électromagnétiques à partir des appareils, est-ce que je me trompe ou bien est-ce que la complexité du nouveau matériel électronique, c'est-à-dire la complexité des puces qui sont devenues beaucoup plus petites et qui exigent beaucoup moins d'énergie, n'a

[Texte]

Mr. P. Lawrence: Absolutely; yes.

Mr. Beatty: So there is some security aspect there.

Mr. P. Lawrence: Right.

Mr. Beatty: Although such... going back to EMP, the more sophisticated, the more susceptible is EMP.

Mr. P. Lawrence: Right.

Mr. I. Henderson: You have to look at the other side too: the detection equipment has become far more sophisticated.

Mr. Beatty: Yes. Going back to the question of legislative constraints, and I recognize that your expertise is in the technological field, but what do you see as the need, if any, for legislative protection of information stored in computers? Do you view it as strictly a technological problem or is there a legislative component to it?

Mr. P. Lawrence: You are right in pointing out our expertise as being primarily technical. It is a very difficult question for us to discuss that. From a personal point of view, I think the definition of the problem has to be addressed rather than what legislation will protect against that problem, and the definition of the problem has to be defined. I think in reading the testimony so far, and trying to look at the problems the committee is facing, it is obvious to me that the definition of what is being stolen, if that is what the primary definition has to reach, could resort back to this method of using the electromagnetic spectrum as a reference point.

If you break into an office and take somebody's documents and you physically carry the documents out, how do you define photocopying those documents and taking them? Is the document—you have taken a photocopy, is that stealing something? How do you define talking to somebody else on that telephone and just telling them what you have seen in that office? You have carried nothing in; you have carried nothing out. Photographing what was in that office, or using a facsimile equipment, and just transmitting the documents out and leaving the documents there, you have not taken anything; but you have images, you have information. The documents that you photocopy, transmit, photograph, or talk-out, are using some form of electromagnetic spectrum, whereby you are transferring the image in some way... —using the telephone, you are transmitting it; photocopying, you are using some method of transmitting on the light spectrum within the photocopier.

If you are using a photocopy that you then carry out, you have done the same thing. If you are transmitting on a facsimile machine, you are using a telephone line... Maybe the definition has to come back to any form of information access that is being withdrawn. And there may be a red herring here, that the actual method of storing it, whether it is

[Traduction]

pas en même temps réduit la quantité d'énergie émise sous forme de radiation?

M. P. Lawrence: Absolument, effectivement.

M. Beatty: Par conséquent, c'est un élément de sécurité.

M. P. Lawrence: Oui.

M. Beatty: Mais pour revenir aux pulsions électromagnétiques, plus la technologie se complique, plus les pulsions deviennent sensibles.

M. P. Lawrence: Précisément.

M. I. Henderson: Mais il ne faut pas oublier qu'en même temps le matériel de détection devient de plus en plus complexe.

M. Beatty: Oui. Pour revenir aux dispositions législatives—et je sais bien que votre domaine, c'est la technologie—à votre avis, quelles sont les mesures législatives de protection de l'information entreposée dans les ordinateurs dont nous avons besoin, si toutefois vous jugez qu'il faut faire quelque chose? Pensez-vous que le problème soit strictement technologique ou bien y a-t-il un élément législatif?

M. P. Lawrence: Vous avez raison quand vous dites que notre domaine est purement technique. Pour nous, il est très difficile de discuter des autres aspects. Personnellement, je pense que la première chose à faire, c'est de définir le problème, cela doit venir bien avant la mise en place d'une législation destinée à nous protéger de ce problème. J'ai lu les témoignages que vous avez entendus jusqu'à maintenant, j'ai essayé de comprendre les problèmes du Comité, et il me semble évident que la définition de la chose volée—si c'est véritablement la première chose à faire—pourrait fort bien nous ramener à cette méthode d'utilisation du spectre électromagnétique comme point de référence.

Si vous entrez dans un bureau par effraction pour y voler des documents, si vous emportez ces documents avec vous, comment définissez-vous la photocopie de ces documents? Si vous n'emportez qu'une photocopie, est-ce que vous volez toujours quelque chose? Quand vous parlez à quelqu'un au téléphone et que vous décrivez ce que vous avez vu dans ce bureau? Vous n'avez rien apporté dans ce bureau, vous n'avez rien sorti de ce bureau, où est le délit? Supposons que vous photographiez des documents dans le bureau, vous ne transmettez qu'une copie, les originaux resteront là. Il n'empêche, vous aurez des images, des informations. Les documents que vous photocopiez, que vous transmettez, photographiez ou emportez avec vous, sont reproduits d'une certaine façon en utilisant le spectre électromagnétique qui vous permet de transposer une image—comme vous «transmettez» une image en la décrivant au téléphone, en photocopiant un document, vous faites une transmission qui passe par le spectre de la lumière à l'intérieur du photocopieur.

Si vous utilisez une photocopie, que vous emportez ensuite avec vous, vous faites la même chose. Si vous transmettez grâce à une machine à fac-similé, vous vous servez d'une ligne téléphonique... En fin de compte, pour définir le problème, il faudra peut-être revenir à la définition de l'accès à l'information obtenue. Il faudrait également éviter de s'égarer, car la

[Text]

a piece of paper—that is a storage device. It just happens to be several hundred years old. That is purely a store and forward. I have written it; I have stored it, and I can pass it around and get it back. If you look at it from that point of view, then the computer storage system has to be considered in that way too.

Mr. Beatty: I agree, over the long span, that the broad issue is: What do you do to protect the integrity of information, whether stored in manually accessible form or in electronic form? The time needed to grapple with an issue like that would be years though, and, in the short term, what we have is a vulnerability of information stored in electronic form.

There are deep concerns on the part of individuals on whom information is stored or who depend upon the quality of information stored. There is also deep concern on the part of institutions doing the storing. They are extremely vulnerable and there is a large hole in the law that will allow a person with impunity to access computer-stored information and to misuse it. I think the argument being made by the people in the industry is that rather than worrying about some of the broad philosophical issues related to information per se—is it property, who owns it, and so on—some action has to be taken to close off the loophole directly as it relates to computers, which draws me more and more to the argument that has been made to the committee, that perhaps what we should be doing is have legislation that is as simple as possible at this point, perhaps dealing with computer trespass, if you like, and unauthorized access to computerized information.

Mr. P. Lawrence: Then how do you deal with the example where General Motors, IBM, or Imperial Oil are operating their computers—whether it is in payroll, personnel data, or in computer-aided design—in designing the next year's car styling? That equipment is radiating; nobody has accessed the computer.

Mr. Beatty: I suppose you deal with it the same way you deal with pay-TV; it appears to be a criminal offence to put a filter on your line that will decode the pay-TV. Notwithstanding the fact that the signal is being pushed in on the line, it is the act of decoding that is the offence at the present time.

Mr. P. Lawrence: Except that the equipment originating that transmission is purposely being operated to generate the transmission down that line. There is a purposeful move to do that. In the other comparison, there is no intent to transmit it.

[Translation]

méthode d'entreposage, qu'il s'agisse d'un morceau de papier... ça, c'est un moyen d'entreposage de l'information. La seule différence, c'est qu'il est vieux de plusieurs centaines d'années. C'est un simple moyen d'entreposage et de transmission de l'information. C'est moi qui ai écrit cela, j'ai entreposé une information, je peux maintenant la distribuer et même la récupérer. De ce point de vue-là, le système d'entreposage par ordinateur doit suivre les mêmes règles.

M. Beatty: Je suis d'accord à long terme, le véritable problème est le suivant: que faut-il faire pour protéger l'intégrité de l'information, quelle soit entreposée sous une forme manuelle ou sous une forme électronique? Cela dit, pour véritablement cerner le problème, il faudrait des années et, en attendant, les informations qui sont entreposées dans un appareil électronique sont très vulnérables.

Les particuliers qui sont le sujet de cette information entreposée, les gens qui dépendent de la qualité de l'information en question, s'inquiètent particulièrement de cette situation. Les institutions qui effectuent l'entreposage ont également de profondes inquiétudes. Elles se sentent particulièrement vulnérables et la loi a de grandes lacunes qui permettraient à une personne d'obtenir des données informatiques et d'en abuser en toute impunité. Je pense que les gens dans l'industrie partent plutôt du principe qu'au lieu de se poser des problèmes à propos de l'une ou l'autre grande question philosophique relative à l'information proprement dite, qu'il s'agisse par exemple de la propriété, il faudrait au contraire prendre des mesures qui nous permettraient de fermer une fois pour toute la petite porte, ce qui m'amène de plus en plus à défendre l'argument, qui a déjà été soumis au Comité, selon lequel ce qu'il nous faudrait, c'est une mesure législative aussi simple que possible pour l'instant, mesure qui porterait par exemple sur l'utilisation non autorisée de l'ordinateur, mettons, et sur l'utilisation non autorisée des données informatiques.

• 1150

M. P. Lawrence: D'accord, mais à ce moment-là, que faites-vous dans le cas de General Motors, d'IBM ou d'Imperial Oil qui utilisent leurs ordinateurs pour les feuilles de paie, pour les dossiers du personnel ou même pour la conception informatisée, pour mettre au point disons les lignes de la voiture de l'an prochain? C'est un matériel qui rayonne partout mais personne n'a vraiment accès à l'ordinateur.

M. Beatty: J'imagine qu'on ferait exactement comme dans le cas de la télévision à péage: quiconque installe chez lui un filtre qui lui permet de décoder les signaux de la compagnie de télévision à péage se rend coupable d'une infraction punie par le Code criminel. Même si ce signal est transmis par le câble, à l'heure actuelle, le décodage pirate est effectivement une infraction.

M. P. Lawrence: D'accord, mais il n'empêche que ce matériel qui crée ce signal est bel et bien utilisé pour transmettre ce même signal grâce au câble. Il y a une intention délibérée à l'origine alors que, dans l'autre cas, la transmission n'était pas prévue.

[Texte]

Mr. Beatty: In either case there is no intent to have it received by the individual receiving it and decoding it. The same would apply for pay-TV by microwave in the U.S., where it has been successfully prosecuted when individuals have bought antennas. It was intended that the signal be put out there, but it was put out there for reception by specific individuals who had properly paid for the right to decode it. It would seem to me that perhaps the way to get at that would be in looking at whether or not a person was the intended recipient of information, or whether he had received information he should not have had.

Do you know—and perhaps we should do some research—how the law deals with a telephone tap that did not involve a physical tap on the line, but which dealt with picking up electromagnetic radiation?

Mr. I. Henderson: How do you detect it?

Mr. Beatty: Assuming that you do catch somebody who is prosecuted.

Mr. I. Henderson: I would say that the odds are very, very low that it would be detectable, and I think it would be very, very difficult to prosecute.

Mr. P. Lawrence: I think he was asking specifically for something else there. You could pick up a particular phone conversation by a method of inductive coupling, not attaching it to the phone lines but purposely getting near to it to induce a result, which I think was your question, that there was a purposeful input.

Mr. Beatty: We could perhaps follow up with the Department of Justice on that, but I would think that was prosecutable under wiretapping.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore): Only if it were being used overtly for that very thing—for wire-tapping to be used as evidence in a trial or something.

Mr. Beatty: No. I would imagine that if it were simply curiosity on my part—and again I suppose there is speculation on my part—but if I were simply curious about what you were saying on your telephone, and I were to arrange to intercept your telephone messages, whether I put them to any specific use or not, my guess is that I would be committing an offence.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore): But how would anybody ever know?

Mr. Beatty: There are two issues here. I suppose there is the issue that with a bank robbery if somebody gets away with it, nobody will ever know. But the second issue that the computer people have been concerned with is that assuming you catch the guy red-handed, what can you then do. The complaint various people in the computer community, if you can use jargon like that, have been making is that even if you catch a person red-handed, and you know beyond a shadow of a doubt

[Traduction]

M. Beatty: Mais dans les deux cas, au départ, il n'était pas question que quiconque puisse recevoir l'information et la décoder lui-même. Ce serait la même chose aux États-Unis dans le cas des signaux de télévision transmis par ondes ultra courtes, et d'ailleurs certains particuliers qui avaient acheté des antennes paraboliques ont été poursuivis et condamnés par les tribunaux. Selon l'intention initiale, le signal était effectivement transmis, mais il l'était à l'intention exclusive de certaines personnes qui avaient effectivement payé pour avoir le droit de le décoder. Il me semblerait peut-être logique que nous partions de l'angle du particulier qui était ou non le bénéficiaire prévu; il faudrait peut-être que nous nous demandions si l'information qu'il a reçue, il l'a reçue de plein droit.

Savez-vous, et nous devrions peut-être creuser un peu la chose, ce que la loi prévoit dans le cas d'une écoute téléphonique qui se fait sans dérivation de lignes mais plutôt par captage du rayonnement électromagnétique?

M. I. Henderson: Mais comment le déceler?

M. Beatty: Supposez que vous preniez quelqu'un sur le fait et que vous le poursuiviez.

M. I. Henderson: Je vous répondrai que les chances d'y arriver, les chances que vous puissiez déceler l'infraction, sont extrêmement minimes et que les cas de ce genre seraient extrêmement difficiles à amener devant les tribunaux.

M. P. Lawrence: Mais je pense que la question portait sur autre chose. Il est possible de capter une conversation téléphonique par couplage à induction, sans faire une dérivation de lignes, car il suffit d'être suffisamment proche pour pouvoir utiliser le phénomène de l'induction électromagnétique, et je pense que c'est cela que vous vouliez demander, n'est-ce pas?

M. Beatty: Nous pourrions peut-être poser la question au ministère de la Justice, mais j'imagine que les dispositions législatives relatives à l'écoute électronique permettraient des poursuites.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore): Oui, mais à condition que le procédé soit délibérément utilisé dans ce but, c'est-à-dire l'écoute électronique destinée à étayer un dossier en cas de poursuite.

M. Beatty: Pas du tout. Permettez-moi une hypothèse, supposons que ma curiosité naturelle fasse que j'aimerais bien savoir ce que vous racontez au téléphone et supposons que je m'arrange pour intercepter vos conversations, quelle que soit l'utilisation ou la non-utilisation que je fasse de cette écoute. Il n'en reste pas moins qu'à mon avis, je me rendrais coupable d'une infraction en le faisant.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore): Mais comment pourriez-vous être découvert?

M. Beatty: Il y a deux éléments. J'imagine que si une banque se fait voler au sens large du terme, et si le coupable s'en tire, personne ne le découvrira jamais. Il y a le second problème, qui inquiète les spécialistes de l'informatique, et qui est celui-ci: supposons que vous preniez le type la main dans le sac, que pouvez-vous faire? Ce dont les milieux de l'informatique se sont plaints, c'est que même si vous attrapez quelqu'un en flagrant délit, même si vous savez certainement bien que

[Text]

that was the individual, and even if he confesses that he had accessed this information, it is still not a prosecutable offence. It seems to me that in preparing for our report what we have to do is to find some concept that is sufficiently simple, which we can legislate on the strength of, and perhaps leave some of the more complex issues—such as the status of information as property, ownership of information, and so on—to a later date. Otherwise, we are left in the position where you can have compelling arguments for doing nothing forever.

Mr. P. Lawrence: I think Mr. Rous had some very good references in his presentation regarding the action being the problem to face.

• 1155

Your last point there is comparable to somebody purposely trying to find information by breaking into a building by tapping on wires, direct or induced tapping, or finding some method of getting close to a facility whereby he could detect it, compared with somebody who is not particularly aggressive at coming into a facility but who can sit... because you are radiating at quite a distance away. So there is that problem of your handing out the information too.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Lawrence, you have brought forth today a very interesting approach, which is not really known, I think, by most people who are using word processors and computers and other types of equipment of that nature; I think they all feel, or have, certainly, in the past—most of the people who use them feel the only way you can intercept is actually to have a terminal to hook up to. This new dimension of this unconnected access to information I think is absolutely important—very important for all these people who are users to understand.

When you talk about this unconnected access to information, you bring up what you call your industrial “tempest” program. My understanding, if I understand it correctly, is that this in effect is a kind of screen that you put around the transmission, or the emission of, I suppose, any kind of waves coming from a piece of equipment. I wonder, how do you go about screening the transmission? Is this something that is done by the manufacturer? Are the manufacturers concerned about this? If not, why are they not concerned about it? If that is not the case, then they are not selling a piece of equipment that is secure.

Mr. P. Lawrence: In most instances they are not interested in security, and most customers are not interested in security from that point of view. This is a relatively new subject that has appeared, is it not, from the point of view of a customer realizing that he is vulnerable from an information point of view? So over the last few years industry has not had to pay attention to that, except in a very narrow area, where it is dealing with the security agencies within the government, who

[Translation]

c'est lui le coupable, même s'il avoue son acte, ce n'est pas une infraction qui peut être poursuivie devant les tribunaux. Il me semblerait qu'en vue de notre rapport, nous devons arriver à trouver une notion suffisamment simple qui pourrait servir de base à une mesure législative, quitte à passer sous silence ou à aborder plus tard certains problèmes plus complexes comme la propriété de l'information, par exemple. Si nous ne procédons pas de la sorte, nous risquons de multiplier les arguments, d'ailleurs parfaitement valables, en faveur d'un immobilisme absolu.

M. P. Lawrence: M. Rous avait, dans son exposé relatif aux mesures à prendre en réaction au problème, quelques excellents éléments de référence.

Le dernier argument que vous nous avez présenté revient en fait à comparer le cas d'un individu qui, sciemment, essaie de découvrir des renseignements en s'introduisant dans un immeuble, en faisant des dérivations, c'est-à-dire en captant directement ou indirectement certains signaux, ou en arrivant à se rapprocher suffisamment pour pouvoir capter ce qu'il cherche, au cas de quelqu'un d'autre, plus passif, et qui peut se contenter de rester là... tout cela à cause du rayonnement. Il y a donc également le problème de ce rayonnement des signaux dont vous êtes à l'origine.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Lawrence, vous nous avez fait part aujourd'hui d'une façon très intéressante de voir les choses, façon de voir à laquelle, dirais-je, ne pense pas la plupart des gens qui utilisent, par exemple, des machines de traitement de textes et des ordinateurs, dans la mesure où j'imagine que tous partent du principe ou sont partis du principe jadis, et je parle ici des utilisateurs, que la seule façon de pouvoir capter quelque chose, c'est de pouvoir disposer d'un terminal et de le brancher au réseau. Mais cette nouvelle dimension de l'accès à distance, sans lien matériel, est parfaitement capital, et il est absolument essentiel que tous les utilisateurs en soient parfaitement conscients.

Parlons de cet accès à distance; vous introduisez alors ce que vous appelez votre programme industriel «tempête» qui revient, si j'ai bien compris, à installer autour des lignes de transmission un genre d'écran, un blindage j'imagine, qui arrête la propagation des ondes émanant du matériel. Comment parvenez-vous à blinder également la transmission proprement dite? Le fabricant peut-il y arriver? Est-ce que les fabricants s'intéressent au problème pour commencer; et dans la négative, pourquoi? Si les fabricants n'en ont cure, j'imagine qu'ils mettent sur le marché du matériel qui n'est pas «étanche».

M. P. Lawrence: Dans la plupart des cas, le facteur sécurité ne les intéresse pas et la plupart des clients ne sont pas intéressés eux non plus. Ce sujet est relativement récent, n'est-ce pas, et j'entends par là le client qui se rend compte brutalement qu'il est vulnérable du point de vue de l'information. Dès lors, même tout récemment, l'industrie n'a pas vraiment dû se pencher sur le problème, sauf dans quelques cas extrêmement limités, celui par exemple des organismes et des entités

[Texte]

are probably the only people who initially could afford to look at the expense of getting into this.

As I understand it, last year an approach was made by the federal government to approximately 25 Canadian companies to see if they would enter the tempest industry to create security by becoming a tempest-producing equipment manufacturer. Most of them found that they could not afford to get into that, because of the expense of creating the tempest engineering capability and because their market to sell to would not amortize the cost of investing in this facility. So none of them have in effect taken up that challenge; and that is where we have evolved in the last year, through our knowledge from being on the periphery of the security community, to develop a facility that will be of central engineering excellence here in Canada, probably Ottawa, which is where we are establishing it, to provide a facility whereby we can take Canadian manufactured equipment and tempestize it—make it screened.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you not feel, then, that the engineer who deals with both the electromagnetic interference with the equipment and also the tempest, which is the security aspect of it, should be doing both and not just one or the other? In other words, the statement is made here in this industrial tempest program paper that you have presented us that the engineer in effect is wearing two hats, when most of the time it is either one or the other; he is either concerned about security or he is just concerned about the transmission of information.

Mr. P. Lawrence: Maybe we could go back a bit further. If I am a design engineer putting together a word processor, I probably know nothing about the electromagnetic spectrum of transmission and radio frequency transmission. I probably would have no comprehension of that at all. I am dealing primarily in logic, in microprocessor circuitry, where I am processing information and I am purely looking at my operating programs and my storage programs and my method of presenting the information and of entering it into the machine and of getting printouts.

I have no comprehension, probably, of any form of radiation from that equipment. It is a totally different discipline within the engineering profession. There are very few people in Canada who would understand compromising emanations by definition, electromagnetic radiation or radio frequency interference. Those are very specialized fields.

[Traduction]

soucieuses de leur sécurité au sein du gouvernement, et ce sont probablement dirais-je les seules, qui, dès le départ, pouvaient se permettre financièrement parlant d'envisager sérieusement la chose.

Si je ne me trompe pas, le gouvernement fédéral a pris contact l'an dernier avec environ 25 entreprises canadiennes pour leur demander si elles étaient disposées à faire partie de ce secteur industriel «tempête» et si elles étaient disposées à produire du matériel étanche dans ce domaine. La plupart de ces entreprises ont découvert qu'elles ne pouvaient pas se le permettre, vu la dépense nécessaire pour mettre en place l'infrastructure technique et indispensable et aussi en raison du fait que le marché auquel elles s'adressent ne leur permettrait pas d'amortir leurs frais d'investissement dans ce domaine. Aucune de ces entreprises n'a donc relevé le gant et c'est la raison pour laquelle, l'an dernier, nous avons petit à petit, parce que nous savions que nous étions en quelque sorte aux confins du problème, mis au point une infrastructure qui va être à la fine pointe de la perfection technique au Canada, à Ottawa probablement, car c'est là que nous allons opérer, infrastructure qui nous permettra de rendre «étanche» le matériel informatique d'origine canadienne.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ne penseriez-vous pas que l'ingénieur qui travaille à la fois sur les interférences électromagnétiques et sur le problème de l'étanchéité, c'est-à-dire l'aspect sécuritaire, devrait effectivement travailler dans les deux directions à la fois et ne pas se contenter d'une des deux spécialisations? En d'autres termes, vous nous avez dit que, selon le programme industriel que vous nous avez soumis, votre ingénieur assume effectivement deux rôles, alors que la plupart du temps, il en assume surtout un au détriment de l'autre. Votre ingénieur s'occupe soit de la sécurité, soit de l'acheminement de l'information.

M. P. Lawrence: Nous pourrions peut-être remonter un peu plus loin. Supposons que je sois ingénieur chargé de concevoir une machine de traitement de textes. Il est possible que je sois tout à fait ignorant en matière de spectre électromagnétique et de fréquences radio. C'est un domaine qui, j'imagine, pourrait fort bien m'échapper tout à fait. Ce qui m'intéresse avant tout, c'est la logique, ce sont les microcircuits, là précisément où se fait le traitement de l'information, et je me penche exclusivement sur les programmes d'exploitation que j'ai conçus, sur les programmes de mémorisation que j'ai conçus, sur la méthode d'affichage de l'information que j'ai conçue et sur la méthode de mise en mémoire et d'affichage par imprimante des éléments.

Il est donc probable que je n'y entende absolument rien au rayonnement émis par le matériel. C'est une discipline tout à fait différente du métier d'ingénieur proprement dit. Très rares sont les gens au Canada qui pourraient comprendre ce qu'il en est exactement des émanations, du rayonnement électromagnétique ou de l'interférence des fréquences radio car ce sont des domaines extrêmement spécialisés.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Certainly the manufacturer must know this.

Mr. P. Lawrence: Not necessarily.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You think not.

Mr. P. Lawrence: Because he is not in the transmission field. He is not into radio transmission. He is not into any form of equipment other than the fact that he is dealing in purely binary logic within his circuitries.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): If, then, the purchaser of the equipment has any concerns which, hopefully, they will have in the future after this meeting and others, they are going to want to expect and maybe even demand that the manufacturer provide some kind of a tempest, whatever that really means—the security process . . .

Mr. P. Lawrence: It is a screening process.

The Acting Chairman (Mr. Robinson, Etobicoke—Lakeshore)): . . . yes, the screening security process for the transmissions that would be passed from the equipment, whether directly or indirectly.

Mr. P. Lawrence: The electronics market or the high-tech community is driven by the market opportunities it faces. It is a very expensive method of getting into that marketplace and I do not think many of them understand that market. I do not think there is going to be that amount of comprehension.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): If you can intercept the electromagnetic broadcast, can you also tamper with the broadcast itself?

Mr. P. Lawrence: No. You have to be in the process or in the actual connecting link to be able to go back in and interface with the stored data.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): In other words, you can remove the data, or you can remove the data if it is being processed, but you cannot remove data that is dormant.

Mr. P. Lawrence: That is right—absolutely right.

Mr. Beatty: Yes, you can. That is what EMP is all about.

Mr. P. Lawrence: Oh, that is destruction.

Mr. Beatty: Yes—destruction or removal. You could . . .

The Acting Chairman (Mr. Robinson, (Etobicoke—Lakeshore)): I am thinking of removing it from the point of view of using it, reading it and finding out what is there, not just destroying what is on it.

Mr. Beatty: You could certainly alter data. For example, if there were payroll or customer records kept in a computer, it would be possible by bombarding it with electromagnetic

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Le fabricant, lui, doit être au courant.

M. P. Lawrence: Pas nécessairement.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ah non?

M. P. Lawrence: Non, parce que les transmissions ne sont pas son domaine. Les transmissions radio ne sont pas sa spécialité. Sa spécialité, c'est exclusivement le matériel qu'il construit, c'est-à-dire un matériel basé sur une logique binaire pour ses circuits.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): A ce moment-là, si l'acheteur du matériel se pose des questions, et il est à espérer qu'il s'en posera à l'issue de nos réunions, il est possible qu'il demande, voire qu'il exige, que le fabricant lui fournisse du matériel qui soit étanche, pour la sécurité . . .

M. P. Lawrence: Il s'agit d'un blindage.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): . . . c'est cela, il voudra que tout ce qui sort directement ou indirectement de son matériel soit arrêté par une forme de blindage.

M. P. Lawrence: Le marché de l'électronique ou de la technologie de pointe est mû par la loi de la demande. C'est un marché qu'il est extrêmement coûteux de pénétrer et je ne pense pas qu'ils soient nombreux à bien comprendre ce marché. Je ne pense pas que cette notion soit si bien comprise que cela.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): S'il est possible d'intercepter une onde électromagnétique, peut-on également la modifier?

M. P. Lawrence: Non. Pour le faire, il faut effectivement pénétrer les circuits, matériellement j'entends, c'est-à-dire pouvoir disposer d'une interface qui vous donne accès à la mémoire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): En d'autres termes, il est possible de subtiliser les données ou d'éliminer les données pendant leur traitement, mais il est impossible de subtiliser des données en veilleuse.

M. P. Lawrence: C'est tout à fait exact.

M. Beatty: Pas du tout. Que faites-vous de la PEM?

M. P. Lawrence: Oui, mais cela c'est de la destruction pure et simple.

M. Beatty: Oui, de la destruction ou de la subtilisation de données. Il est possible . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Quand je parle de subtiliser ou d'éliminer des données, je pense à l'utilisation, au déchiffrement et à l'acquisition en quelque sorte de ces données et non pas simplement à leur destruction.

M. Beatty: Il n'empêche qu'il est possible de modifier des données. Ainsi, supposons une mémoire informatique dans laquelle sont stockés des dossiers de client ou des feuilles de

[Texte]

waves to damage the information stored in there. Indeed, that is what EMP would do.

Mr. P. Lawrence: Or you could go in with a hand magnet and destroy it. This is a steam engine method of entering into the system, is it not? But the chairman was asking specifically would this unconnected remote access to the information... can you interface with the equipment, can you have an intelligent conversation? No, you cannot, because then you are getting into the other submissions you have had regarding breaking codes and interfacing with equipment, which we have not been addressing.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So what you are really talking about is this unconnected access; but it is only to information which is at being radiated at that time.

Mr. P. Lawrence: By processing it, printing it, entering it, or transmitting it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes. And if none of these things are happening, then of course you could not enter the data bank. You could not get the information.

Mr. P. Lawrence: You would not be able to hear anything, because nothing is being radiated; that is true, sir.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Now what is the cost involved in this to provide the kind of security you feel would be necessary?

Mr. P. Lawrence: For protection?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes.

Mr. P. Lawrence: You are probably looking at a price increase of a word processor from 50% to 75% of the standard product price.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You talked about a screen. What kind of screen are you talking about? Is it a high frequency screen or...

Mr. P. Lawrence: No, no, sorry. The screen would be a metal screen.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I see.

Mr. P. Lawrence: The simplest definition would be to put the equipment in a very thick metal box, very heavy, very difficult to move around; but it would be screened because it would not be able to radiate through the box. There is one article there with a very large picture on top which shows you this metal cladding around some equipment to protect it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose with the technology we have today it

[Traduction]

paie, il est toujours possible, par un bombardement électromagnétique, de brouiller les données qui sont mises en mémoire, et c'est ce qui se produirait d'ailleurs si on utilisait la PEM.

M. P. Lawrence: Il suffirait simplement de promener un aimant au-dessus des mémoires pour les détruire. Ce serait une façon assez archaïque de jouer avec un système, ne pensez-vous pas? Quoi qu'il en soit, le président me demandait précisément si cette acquisition à distance sans lien matériel de l'information... pouvez-vous établir une interface avec le matériel, pouvez-vous converser intelligemment avec lui? Non, parce qu'à ce moment-là il faudrait que vous ayez déchiffré les codes et que vous ayez effectivement une interface, et ce n'est pas là ce dont nous avons parlé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Donc vous limitez votre propos à l'accès indirect, à distance; mais à ce moment-là, vous n'acquerez que les données qui sont transmises, et vous les obtenez grâce au rayonnement.

M. P. Lawrence: Lors du traitement, de l'impression, de la mise en mémoire ou de la transmission.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): C'est cela. Et, il est certain que si aucune de ces opérations ne s'effectue, il vous est impossible de vous introduire dans la mémoire. Les données à ce moment-là vous échappent.

M. P. Lawrence: Il vous est impossible de percevoir quoi que ce soit, car il n'y a pas de rayonnement, vous avez raison.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Cela étant, à combien chiffreriez-vous la dépense pour arriver à «impermeabiliser» le matériel selon vos critères?

M. P. Lawrence: L'imperméabilisation?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): C'est cela.

M. P. Lawrence: Dans le cas d'une machine de traitement de texte, on pourrait sans doute envisager une augmentation du prix courant de l'ordre de 50 à 75 p. 100.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé d'un blindage. De quoi s'agirait-il au juste? S'agit-il d'un blindage des hautes fréquences...

M. P. Lawrence: Excusez-moi, il s'agirait effectivement d'un blindage métallique.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'accord.

M. P. Lawrence: La façon de procéder la plus simple consisterait à enfermer tout le matériel dans un coffre métallique aux parois très épaisses, un coffre qui serait très lourd et très difficile à déplacer. A ce moment-là, vous auriez imperméabilisation car le rayonnement serait arrêté par les parois du coffre. Vous avez ici un article avec la photo qui vous montre ce blindage métallique qui entoure certains appareils pour les protéger.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'imagine qu'avec la technologie actuelle, il ne

[Text]

would not be very long before even that kind of a screening system would not be operative or successful. Yes?

Mr. I. Henderson: If it has been approved under NASCIM 5100A, which is the NSA definition, then it is very difficult to tell whether or not the equipment is on or off. That is about the only compromising signal that will come out.

• 1205

The Acting Chairman (Mr. Robinson (Etobicoke... — Lakeshore)): The National Security Agency of the United States then has a continuing program of what you would call, I suppose, their tempest program, their industrial tempest program. Is that all-encompassing, or is there more to it than that?

Mr. P. Lawrence: I do not understand the question.

Mr. I. Henderson: I think what you are looking at is the NSA has rules and regulations on testing equipment and to test whether or not there are any compromising emanations from the equipment. At the same time, they also have certain design guidelines on how to design the equipment, and that is when you are getting into some more of the expense. But their industrial tempest program is sort of a need-to-know basis. If you want to supply the U.S. federal government or the Canadian government or some of the NATO countries with this type of equipment and you have a contract to supply some of the tempestized equipment, then you are permitted to join the industrial tempest program. The program is designed to encourage companies to get in and start working on the tempest problem.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): And does this tempest program also include a backup or a way of testing the efficiency or the security of the program?

Mr. I. Henderson: There is quality control. One of the references there to the NASCIM 5100A—those are the rules and regulations for testing the equipment, and on a quality control basis usually one out of 20 or one out of 10 will be picked off the line and tested for this type of emanation.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose it would be fair to say that today no conversations are really secret.

Mr. I. Henderson: Never say anything on the telephone that you do not want to see on the front page of the paper tomorrow morning.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose we are really getting back into the horse-and-buggy days where we should communicate by writing it on a piece of paper and having it delivered by a horseman or the pony express or something.

Mr. I. Henderson: As long as you are within line of sight. Even sitting in this room, somebody up to five miles away with

[Translation]

faudrait guère de temps pour qu'un tel blindage puisse être effectivement utilisable. Me trompais-je?

M. I. Henderson: S'il a reçu l'homologation de la NSA dans le cadre de la norme NACIM 5100A, à ce moment-là il serait très difficile de dire si un équipement ainsi blindé est ou non en circuit, car c'est là à peu près le seul signal compromettant pouvant sortir d'un appareil blindé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): La *National Security Agency* américaine a instauré un programme, un programme permanent qui est je crois le programme *tempest*, programme d'imperméabilisation industrielle. S'agit-il d'un programme global ou y a-t-il autre chose?

M. P. Lawrence: Je n'ai pas compris votre question.

M. I. Henderson: Vous voulez, je crois, parler du fait que la NSA a des règles et des règlements pour tester du matériel, ce qui permet de déterminer si le matériel en question émet ou non un rayonnement compromettant. Il y a également certaines directives de la NSA en matière de conception du matériel, et c'est là où cela commence à coûter plus cher. Mais le programme industriel *tempest* est en quelque sorte un programme portant sur l'acquisition de tous les éléments qu'il importe de connaître. Si vous voulez fournir du matériel au gouvernement américain, au gouvernement canadien ou à certains États membres de l'OTAN, si votre contrat porte sur la fourniture de matériel étanche, à ce moment-là, vous faites automatiquement partie du programme *tempest*. Ce programme a pour but d'encourager les compagnies à y adhérer et à commencer à se pencher sur le problème du blindage.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ce programme s'assortit-il également d'une composante de vérification qui vous permet d'assurer le blindage du programme lui-même?

M. I. Henderson: Il y a le contrôle de la qualité. On a parlé de la norme NASCIM 5100A—il s'agit de la réglementation relative aux essais du matériel, et pour ce qui est du contrôle de la qualité, je dirais qu'un appareil sur 20 ou un appareil sur 10 est régulièrement prélevé de la chaîne de montage pour faire l'objet d'une vérification des rayons indésirables.

Le président suppléant (M. Robinson (Etobicoke-Lakeshore)): J'imagine qu'on peut dire sans guère risquer de se tromper qu'à l'heure actuelle aucune conversation n'est vraiment secrète.

M. I. Henderson: Lorsque vous êtes au téléphone, ne dites jamais rien que vous ne voudriez pas voir faire la manchette des journaux le lendemain matin.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'imagine que nous en revenons petit à petit au bon vieux temps où nous communiquions par écrit et où le pli était livré par messenger à cheval...

M. I. Henderson: Cela vaut pour tous les cas où vous êtes à portée optique. Nous sommes assis ici dans cette salle, mais

[Texte]

a laser can be bouncing it off the window and the window is acting as a speaker and there is an intelligible signal going out.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So everything we are saying in this room right now could be transmitted just through a laser beam, say, over to Hull.

Mr. I. Henderson: Exactly.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): What, then, could be done to stop this? Would we have to hold our hearings in a metal box?

Mr. I. Henderson: That is what embassies in sensitive areas use. They will have a room that is suspended and is acoustically clear and is swept; it is designed so nothing that is said in that room will get out.

Mr. Beatty: We should point out, Mr. Chairman, that a politician's problem is not usually to avoid getting on the front page of *The Globe and Mail*; it is usually seeking to get on it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You spoke about the definition, and I think definitions really are important. Have you considered what might be considered as a definition for "property"? We are talking about computer crime and computer theft, this kind of thing. I think you gave it certain criteria that would have to be followed. You talked about a photocopy, or describing something over the telephone and what you saw in a room, transmitting a document and so on, different ways of doing this; but there has to be a property in it—or do we have to have a new definition for the word "property" in order to effect the legislation?

Mr. I. Henderson: I think any information is property. It depends who is the victim, really. If a private company's data bank is being violated, if somebody is exploiting it or manipulating it, then the victim is the private company. But if the private company is holding, say, the health records of everybody in Canada, or even, say, your income tax return, if that is in the data bank, then more than just one person is a victim; the victims, all of a sudden, are spread out.

Mr. P. Lawrence: It is really the activity itself, because if I happen to read a document that is nationally secure or is private information from somebody's health record or is legal information about a prosecution that took place but is not supposed to be public information, the fact that I have read it and I have stored it in my personal computer, but I am not using it . . . Have I done something wrong by knowing about it? I think Mr. Rous . . . again I am referring to his reference to the level of action. Is it property by ownership?

[Traduction]

quelqu'un pourrait très bien, à cinq milles d'ici, utiliser un laser qui capterait les vibrations de la fenêtre qui est en fait un haut parleur et émet un signal compréhensible, et entendre ainsi notre conversation.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ainsi donc, tout ce que nous disons ici pourrait être transmis mettons à Hull par faisceau laser?

M. I. Henderson: Parfaitement.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Que faire donc pour l'éviter? Devons-nous siéger dans un coffre-fort?

M. I. Henderson: C'est ce que font les ambassades dans les régions troublées. Elles ont une salle spéciale isolée, suspendue et anéchoïque, une salle sourde dont rien ne peut sortir.

M. Beatty: Il est à remarquer, monsieur le président, que le plus souvent, un homme politique tient davantage à faire les manchettes du *Globe and Mail* qu'à y être passé sous silence.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé de la définition, et à mes yeux les définitions ont leur importance. À vos yeux, que pourrions-nous envisager comme définition de la «propriété»? Nous parlons du délit informatique, nous parlons du vol informatique, et je pense que vous avez avancé certains critères qui devraient être respectés. Vous avez parlé de photocopie, vous avez parlé des entretiens téléphoniques, vous avez parlé de l'acheminement des documents et des diverses façons de procéder, mais il est certain qu'il y a une motion de propriété dans tout cela. Devrions-nous refaire la définition du mot «propriété» pour arriver à légiférer?

M. I. Henderson: Selon moi, tout renseignement est une propriété privée. Evidemment, tout dépend de qui est la victime. Si la mémoire informatique d'une entreprise est «sucée», exploitée ou manipulée par un tiers, à ce moment-là, c'est l'entreprise qui est la victime. Mais supposons que cette entreprise ait en mémoire les dossiers médicaux de tous les Canadiens ou encore les dossiers fiscaux de tous les Canadiens, à ce moment-là, vous multipliez le nombre de victimes et tout d'un coup, c'est toute la population qui est la victime.

M. P. Lawrence: En fait, il faut considérer l'activité proprement dite car, admettons que je mette par hasard la main sur un document couvert par le secret d'État ou sur un document qui contient des renseignements confidentiel à propos de l'état de santé de telle ou telle personne, voire sur un document juridique relatif à des poursuites et qui contient des données qui ne sont pas censées être du domaine public, le seul fait pour moi d'avoir pris connaissance de ce document et de l'avoir mis en mémoire dans mon petit ordinateur, sans pour autant que j'en utilise les éléments . . . Ai-je fait quelque chose de mal parce que je suis au courant? M. Rous . . . et je veux encore une fois parler, comme il l'a fait, du niveau d'intervention. S'agit-il d'une propriété de plein droit?

[Text]

[Translation]

• 1210

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Just so that the record will show exactly what you mean, I wonder if you would describe this again. You talked about your own personal computer and you tapped your head. I do not know whether you mean your brain, or whether it is a personal computer you have as well. You might just explain that.

Mr. P. Lawrence: I am sorry—you are right. I am talking about my brain.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right.

Mr. P. Lawrence: I have stored that information. I have not used it—used the information, I mean, used my brain.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Then how can you determine the victim?

Mr. P. Lawrence: That is the point, I think, to which Ian was referring. If I had taken action with that information that I have, I could cause a problem and the problem is the victim, or the problem is effected on the victim.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): One of the problems we seem to have is that the normal definition of many of the words we are using—say “property”, “victim” and other words—does not seem to have the same meaning, or should not necessarily have the same meaning, when we are talking about a computer crime, the topic that is before us. One of the dilemmas we have is to make the definitions more defining in nature of what we are really talking about, because at some time we are looking toward the preparation of legislation—which brings up another point.

What kind of legislation do we need? Do we need a special act with special definitions for this particular situation, for computers or equipment of that nature, so that they would have one definition generally and a special definition when you are talking about computers? This is one of the dilemmas we have. Can you help us in this at all?

Mr. I. Henderson: Only as far as to think of a . . . There has to be a criminal intent to intercept some form of telecommunications and then the definition of telecommunications has to be expanded to include almost anything on the electromagnetic spectrum. That is where the problem lies.

Mr. P. Lawrence: I think we are trapped in the method we have been talking about technically for the last few years of storing information and holding it. We have been purely looking, as human beings, at what we have in a locked cabinet, or in the house, or a cupboard, or locked away in some definable physical activity or physical location, but that is

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Peut-être pourriez-vous décrire à nouveau la chose, afin que le compte rendu ne laisse aucun doute à ce sujet. Vous avez parlé de votre petit ordinateur personnel, et vous vous êtes frappé le front. Vous parlez de votre propre cerveau ou d'un véritable ordinateur? Pourriez-vous nous l'expliquer?

M. P. Lawrence: Excusez-moi, vous avez tout à fait raison, je parlais de ma propre mémoire, de mon propre cerveau.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'accord.

M. P. Lawrence: J'ai donc mis ces renseignements en mémoire dans ma tête. Je ne les ai pas utilisés, je me suis simplement servi de ma tête.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À ce moment-là, comment pouvez-vous identifier la victime?

M. P. Lawrence: C'est précisément de cela qu'il s'agit, comme le disait, je crois, Ian. Si j'avais fait quelque chose suite à ces renseignements dont je dispose, à ce moment-là, j'aurais pu créer un problème et faire une victime.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Un des problèmes qui semblent se poser à nous vient du fait que la définition normale de bien des termes que nous utilisons, par exemple le mot «propriété», le mot «victime» et j'en passe, ne semble pas avoir la même signification, ou ne devrait pas avoir nécessairement la même signification, lorsque nous parlons d'un crime informatique, c'est-à-dire ce dont nous sommes saisis. L'un des dilemmes qui se posent à nous vient justement du fait que nous devons en arriver à des définitions qui définissent davantage ce dont nous parlons, car, à un moment donné, nous allons devoir nous atteler à la rédaction d'un projet de loi, mais c'est une autre histoire.

De quel genre de mesures législatives avons-nous donc besoin? Il nous faut une loi spécifique, assortie de définitions spéciales correspondant à la situation, correspondant aux ordinateurs et au matériel apparenté, de sorte que nous aurions une définition en général et une définition spécifique valable pour les ordinateurs, est-ce cela? Voilà l'un de nos dilemmes. Pourriez-vous nous aider?

M. I. Henderson: Oui, mais seulement dans la mesure où il s'agit . . . Il doit y avoir, à l'origine, intention délictueuse; il faut que le coupable ait effectivement l'intention d'intercepter une forme ou une autre de télécommunication à des fins délictueuses, et à ce moment-là, il faudrait élargir la définition des télécommunications, de manière à ce qu'elle englobe quasiment tout le spectre électromagnétique. Voilà le problème.

M. P. Lawrence: Je pense que nous sommes pris au piège, un piège dont nous parlons entre techniciens depuis quelques années, et il s'agit du stockage et de la mise en mémoire des données. Nous sommes des êtres humains et nous nous sommes très longtemps contentés d'envisager le cas de ce que nous entreposons matériellement dans une armoire, dans un

[Texte]

purely one of the methods of this process of storing value, of storing property—whatever that is.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): To try to uncomplicate this, at some time we have to get down to the point of recommending some form of legislation, whether it is a special act that would apply to this whole matter or whether it would be an amendment, say, to the Criminal Code. You gentlemen may or may not be lawyers, but you have talked about criminal intent and intent generally, and so on, as though we were saying if there is not criminal intent there is no crime, when we are talking about computer crime as such. But that does not mean that some act has not taken place, whether overtly or covertly, whether directly or indirectly. Because of the kinds of things we are dealing with, it can happen so easily. There may be no intent at all, but all of a sudden you are getting information on your piece of equipment from somebody else's piece of equipment miles away. So intent may or may not be that important. I really do not have the answer to it. I guess we have to listen to more witnesses, and see if somebody can . . .

Mr. P. Lawrence: You have to be purposely intending to get that information; if it is on your equipment, you have a type of equipment that will detect that information and interpret it, and therefore create a position whereby you have information that could compromise the source.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): It means, in effect, that what you are going to do is say that it is a crime to eavesdrop, regardless of how you do it. You gave an illustration before, that if the door was open and somebody was standing outside he could hear what was going on, and . . .

Mr. P. Lawrence: That cannot be a crime, though, can it, for him to listen?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Let us face it: If you leave the door open, surely as a reasonable man you can expect that somebody might be there and might listen.

Mr. P. Lawrence: If he happens to have the equipment to interpret the transmission—if he happens to have it. In the other sense, for the broadcasting information that is going from a word processor or electronic equipment, he would purposely have to have the detection equipment this time because it is a different level of the spectrum. We are all fitted out with some level of the spectrum; there is a detector called an ear, but that is a very narrow portion of the frequency range.

[Traduction]

classeur, dans un bâtiment, bref, de quelque chose de très matériel, mais il n'empêche qu'il ne s'agit que d'une des nombreuses méthodes par lesquelles nous pouvons emmagasiner ou stocker quelque chose qui a une certaine valeur, un bien, si vous voulez.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans un souci de simplification, il est certain qu'à un moment donné, nous devons en arriver à recommander une mesure législative, ou une autre, qu'il s'agisse d'une loi spécifique qui s'appliquerait à tout ce secteur, ou d'un amendement, mettons, au Code criminel. Vous n'êtes peut-être pas juristes, messieurs, mais il n'empêche que vous nous avez parlé de l'intention délictueuse et de l'intention proprement dite, comme si nous disions que, s'il n'y avait pas intention délictueuse au départ, il n'y a pas de crime ou d'infraction, du moins en ce qui concerne l'ordinateur. Cela ne veut toutefois pas dire que quelque chose ne s'est pas produit, que quelqu'un n'a pas fait quelque chose ouvertement ou non, directement ou indirectement. Dans le domaine que nous étudions, tout cela est tellement facile. Même s'il n'y a pas intention au départ, il se peut fort bien qu'à un moment donné, quelqu'un qui dispose d'un appareil quelconque capte sur son appareil des données qui appartiennent à quelqu'un d'autre, même très loin. Dès lors, cette intention est peut-être importante, mais elle ne l'est peut-être pas non plus. C'est une réponse que j'ignore. J'imagine que nous devons entendre d'autres témoins, pour voir si, peut-être, quelqu'un ne pourrait pas . . .

M. P. Lawrence: Il faut que vous ayez nourri sciemment l'intention d'obtenir cette information. Si ces données apparaissent tout d'un coup sur votre appareil, il est certain que votre appareil vous permet de capter les données, de les interpréter, et dès lors, vous met en mesure d'en compromettre la source.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ce qui signifie, en clair, qu'il nous faut préciser que toute écoute, quelle qu'en soit l'acception et quelles qu'en soient les modalités, est un acte criminel. Vous avez donné un exemple, vous avez dit que si la porte de la salle est ouverte et si quelqu'un se tient dans le couloir et prête l'oreille, il peut entendre ce qui se passe . . .

M. P. Lawrence: Évidemment, ce n'est pas un crime d'entendre?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais soyons réalistes: si vous laissez la porte ouverte, il est certain qu'un homme comme vous, doué de raison, peut s'attendre à ce que quelqu'un d'autre passe par là et prête l'oreille.

M. P. Lawrence: À condition qu'il ait le matériel nécessaire pour interpréter l'émission, à condition qu'il l'ait. Dans l'autre acception du terme, lorsqu'il s'agit des ondes qui émanent d'une machine de traitement de textes ou d'un appareil électronique quelconque, il faudrait, à ce moment-là, qu'il se soit, à dessein, muni du matériel de captage nécessaire, puisqu'il s'agit d'une fréquence du spectre tout à fait différente. Nous pouvons tous capter certaines fréquences du spectre, nous disposons tous d'un détecteur qui s'appelle

[Text]

Mr. I. Henderson: Perhaps the mere acquisition of the equipment to intercept is evidence of criminal intent.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes, it is like having burglary tools, I suppose.

Mr. I. Henderson: Precisely.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): If you are caught with burglary tools, the onus seems to shift to the accused to show that he did not have those tools for burglary, but he had them to fix a light or . . .

Mr. I. Henderson: A screwdriver at noontime is not the same as a screwdriver at 11.00 p.m.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Of course, he would have to explain that he was not going to break into something or jimmy a window open, but rather was carrying it for protection or something.

Anyway, I wanted to ask you about one thing. You gave an illustration about the truck going around the community and testing the TV signals to find out not only that a TV was on but that a particular channel was on. This is quite devious, to say the least. But I note from one of the papers here that in Great Britain, if you have a television set you are taxed. I have about half a dozen television sets, I guess, in various places—in my apartment, in my office, in my house, and so on. It would be a tremendous amount of tax you would probably pay. Fortunately for us, Canada has not gotten around to the point of taxing your television set, maybe the size of the set, whether it is coloured or black and white or what not. If that happened, then the truck would be going around to find out whether or not people have clandestine television sets and whether or not they are paying the tax; and they could tell.

Mr. I. Henderson: That is right, they do that.

Mr. P. Lawrence: They are doing that or have done it for years.

Mr. I. Henderson: In West Germany, several weeks ago there was a program—I think it was worldwide, on the CBC—on a Saturday afternoon. They were talking about the problem in West Germany of trying to track down who has unlicensed TV sets. They showed an intercept truck going around; and the intercept truck could come up with a map on the screen to

[Translation]

l'oreille, mais qui ne nous permet de capter qu'une gamme de fréquences du spectre qui est extrêmement limitée.

• 1215

M. I. Henderson: Peut-être le simple fait de se procurer le matériel d'interception nécessaire serait-il la preuve d'une intention délictueuse.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui, un peu comme le fait d'avoir en sa possession une trousse de cambriolage, j'imagine.

M. I. Henderson: Exactement.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Si on vous prend sur le fait avec, en votre possession, une trousse de cambrioleur, j'imagine que ce serait, à ce moment-là, à vous à prouver que vous n'aviez pas cette trousse pour perpétrer un cambriolage, mais bien pour réparer une lampe, ou je ne sais quoi.

M. I. Henderson: En plein jour, un tournevis n'est pas le même outil qu'à minuit.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): C'est évident, et son détenteur devrait, à ce moment-là, expliquer qu'il n'avait pas sur lui un tournevis pour forcer une fenêtre ou une porte, mais plutôt, par exemple, pour se protéger.

Quoi qu'il en soit, j'aimerais vous poser une autre question. Vous avez parlé de ces camions qui servent à décoder les signaux de télévision et à découvrir non seulement qui possède un poste de télévision, mais qui écoute telle ou telle chaîne. C'est un procédé pour le moins un peu douteux. Je relève pourtant dans l'un de nos documents qu'en Grande-Bretagne, les récepteurs de télévision font l'objet d'une taxe spéciale. J'ai personnellement une demi-douzaine, environ, de postes de télévision, chez moi, au bureau, dans mon appartement, et ainsi de suite. J'imagine qu'en Grande-Bretagne, cela me coûterait extrêmement cher en taxes. Heureusement pour nous, le Canada n'en est pas encore arrivé à imposer une redevance annuelle par récepteur de télévision, une redevance qui, j'imagine, pourrait être calculée selon les dimensions du récepteur, selon qu'il s'agit d'un récepteur noir et blanc ou d'un récepteur couleurs. Si nous en arrivons jamais là, j'imagine que ces camions pourraient nous permettre de découvrir si, effectivement, les gens n'ont pas des récepteurs de télévision clandestins pour lesquels ils n'acquittent pas la redevance.

M. I. Henderson: C'est tout à fait cela, et c'est de cette façon qu'on procède.

M. P. Lawrence: Et cela fait des années.

M. I. Henderson: Il y a quelques semaines, c'était un samedi après-midi, je crois, une émission est passée sur l'antenne de Radio-Canada, émission qui a été diffusée, je crois, dans le monde entier, et qui parlait de l'Allemagne occidentale, qui essayait de repérer les postes de télévision clandestins. On pouvait voir un camion qui faisait sa tournée et l'écran sur lequel il captait les ondes des récepteurs de télévision et grâce

[Texte]

show precisely where on the block these unlicensed TV sets were, because the TV set does give off a signal.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right. That being the case, you would have to have a tempest program for each and every television set, or watch your television in a . . .

Mr. P. Lawrence: But you have nothing to protect. You are not transmitting anything on that about which you have any concern, unless you happen to have the cablevision now detecting a lot of operations within your house because you are away. It is measuring the humidity and it is measuring your tax report, and you are doing your interaction privately with your accounts and your health records. Maybe there is some information there you would worry about, but basically there is nothing on that television you would want to hide from anybody.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Of course there is; you do not want the government to know you have one.

Mr. P. Lawrence: Yes, and pay tax. That is right.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So how do they know if you have more than one, and do they know how many you have if they are not turned on?

Mr. I. Henderson: No, it has to be on.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): There would be nothing emanating from the television set unless it were turned on.

Mr. I. Henderson: That is right.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right. Could they tell if you have more than one?

Mr. I. Henderson: Yes.

Mr. P. Lawrence: You might have it on different programs. Each channel has a different radiating frequency; that is how you separate the channels in your detector.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So they would know how many television sets you have in your house—how many are on, that is, if they are on—and even the programs you are watching?

Mr. I. Henderson: Yes.

Mr. Beatty: I think, Mr. Chairman, we can speak closer to home; that is, the cable companies themselves are very concerned about unauthorized equipment to decode pay TV. They have talked about the possibility of putting vans onto the streets to see whether or not individuals have not paid for pay TV or have decoders on, because they would be emanating radio frequency. They would be able to tell from the street

[Traduction]

auquel le personnel pouvait, en se servant d'une carte du quartier, découvrir leur provenance.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Parfait. À ce moment-là, il faudrait avoir un programme du genre «tempest» pour chaque récepteur de télévision, ou encore, il faudrait regarder la télévision dans un local blindé . . .

M. P. Lawrence: Mais dans ce cas-là, vous n'avez rien à protéger, car vous n'émettez rien qui puisse vous inquiéter, à moins, bien sûr, que le télédistributeur puisse, par le câble, surveiller votre maison et ce qui s'y passe en votre absence, en mesurant le taux d'hygrométrie, en analysant votre formule d'impôt, en surveillant vos comptes en banque et vos dossiers médicaux. Peut-être, à ce moment-là, y a-t-il l'un ou l'autre renseignement qui vous mette mal à l'aise, mais je dirais que dans l'ensemble, personne n'a quoi que ce soit à cacher à quiconque au niveau du récepteur de télévision.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Au contraire, ce que vous voulez, c'est que le gouvernement ignore que vous avez un récepteur de télévision.

M. P. Lawrence: Bien sûr, pour ne pas payer la redevance. Vous avez raison.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Comment peut-il donc savoir si vous en avez plusieurs, surtout s'ils ne sont pas branchés?

M. I. Henderson: Il est certain que le récepteur doit être branché pour pouvoir être décelé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Si le récepteur n'est pas branché, il ne dégage aucun rayonnement.

M. I. Henderson: C'est exact.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'accord. Mais peut-on savoir si vous en avez plusieurs?

M. I. Henderson: Oui.

M. P. Lawrence: Il suffit que chacun d'eux soit branché sur une chaîne différente. Chaque chaîne rayonne sur une fréquence différente, et c'est de cette façon que le détecteur fait la distinction.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Donc, il est possible de savoir combien de récepteurs de télévision vous possédez, ou plutôt, combien de récepteurs sont branchés, de même que les chaînes que vous regardez?

M. I. Henderson: C'est exact.

M. Beatty: Nous pourrions, j'imagine, monsieur le président, cerner un peu plus le problème immédiat, dans la mesure où les compagnies de télédistribution sont elles-mêmes très inquiètes de la prolifération des décodeurs clandestins pour la télévision à péage. Ces compagnies ont elles-mêmes envisagé la possibilité de faire circuler une flotte de camionnettes pour détecter les décodeurs illicites, ou les cas de réception illicite

[Text]

whether, in fact, you had an unauthorized reception of a pay TV signal.

Mr. I. Henderson: Every piece of equipment has its own voice, so that an intercept truck going by, once they have identified that there are three television sets on, can tell you when they come by again which one is watching which channel. They can say the one in the bedroom is watching channel four, once they can identify where it is, because it is going to radiate at a slightly different frequency.

Mr. Beatty: They use a different technology. Bell Canada for years has had the ability to tell whether or not you had an unauthorized extension phone put in. But they did not have a...

Mr. P. Lawrence: It was just measuring the impedance on the line.

Mr. Beatty: Exactly.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): What position would you like the committee to take with regard to the problem of the broadcast information from computer terminals?

• 1220

Mr. P. Lawrence: I think the committee could take the position of suggesting that a formal study be undertaken with regard to problems that exist where terminals are being accessed with resulting loss of revenue, loss of business, or loss of information.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you feel that there should be a requirement that the owner of the equipment have a security program or get involved in this industrial tempest program, as it is called?

Mr. P. Lawrence: It would depend on what the owners of the equipment were processing. If the owners of the equipment were processing your income tax return, perhaps you might feel that equipment should be secure. If they were processing health information, perhaps that should be secure too. But if they were processing their five year plans on what they planned to do with the company, who would be the victim there? It would be the company itself.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, what about the competitors?

Mr. P. Lawrence: There is a lot of attention being paid by industry generally, especially the banking industry and the rest of the finance houses and the legal industry and the medical industry. They are looking at this problem of protecting the information. Unfortunately, they are not very well informed as to how to protect it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): What is your recommendation as to the kind of protection that should be required?

[Translation]

des signaux de télévision à péage, puisque, dans les cas de ce genre, il y aurait des rayonnements hertziens. A ce moment-là, les compagnies pourraient découvrir de l'extérieur qui capte abusivement les signaux de la télévision à péage.

M. I. Henderson: Chaque appareil a sa propre voix, de sorte qu'un camion-gonio pourrait, par triangulation, déterminer qu'il y a trois récepteurs branchés et quelles sont les chaînes sur lesquelles ils sont branchés. Les préposés pourraient, par exemple, dire que le récepteur de la chambre à coucher est branché sur la chaîne quatre, parce que cette chaîne émet un rayonnement légèrement différent.

M. Beatty: La technologie est différente. Cela fait des années que Bell Canada peut découvrir les récepteurs téléphoniques auxiliaires illicites, sans pour autant...

M. P. Lawrence: Il s'agit simplement de mesurer l'impédance de la ligne.

M. Beatty: C'est cela.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À votre avis, quelle serait la position que nous devrions adopter à propos du problème des données émanant des terminaux d'ordinateur?

M. P. Lawrence: Je crois que le Comité devrait proposer qu'une étude officielle soit faite portant sur les problèmes qui existent là où un accès au terminal entraîne des pertes de revenu, d'affaires ou de renseignements.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Croyez-vous qu'on devrait exiger que le propriétaire de l'équipement ait aussi un programme de sécurité ou se prévale de ce programme industriel «tempest», comme on l'appelle?

M. P. Lawrence: Tout dépend des données que traitent les propriétaires de l'équipement. Si les propriétaires de l'équipement devaient traiter votre rapport d'impôt, peut-être alors voudriez-vous que l'équipement soit imperméabilisé. S'ils traitent des données sur la santé, peut-être devrait-on aussi l'imperméabiliser. Mais s'ils traitaient de plans quinquennaux touchant l'avenir de la compagnie même, qui alors serait la victime? Ce serait la compagnie elle-même.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Et les concurrents.

M. P. Lawrence: L'industrie, en général, est très attentive de ce côté-là, surtout lorsqu'il s'agit de l'industrie bancaire et des autres institutions financières, sans oublier les professions juridiques et médicales. Tous essaient de trouver une solution à ce problème de protection des renseignements. Malheureusement, tous ne sont pas toujours bien informés sur la façon de bien faire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'après vous, quel genre de protection devrait-on exiger?

[Texte]

Mr. P. Lawrence: One of the problems that exists is the legislation, within the framework of the government, regarding the permission within the government departments to consider different levels of protection. As I understand it—and I am not a lawyer—the present conditions are such that, if there is anything else but clear definition of information—whether it is confidential, secure, secret, private, anything else but clear—then if it has to be attended to from a secure point of view, it has to be attended at full national security specifications, which is tempest and crypto. It is prohibitive, it is expensive, it is difficult to get the equipment; a lot of people still do not know about it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You fellows prefaced your remarks today by saying that you were suppliers of security equipment to the federal government. Do you feel that we do have sufficient security? Should there be more security? What should we be doing that we are not doing? Finally, can you recommend any kind of legislation that we should pass? Or do we have security legislation now that is satisfactory?

Mr. P. Lawrence: May I go back? We did not say we supplied secure equipment, sir. We must define that. We supply electronics and telecommunications equipment to the security community. We provide equipment that meets tempest specifications. The definition of security equipment sometimes is interpreted to mean crypto, or the equipment that would provide security. There are some definitions in there which I think the communications security establishment would be very good for sourcing and defining. But we do not claim to provide security equipment. We provide equipment that will go into a security environment that has been tempestized. I must define that.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Maybe a distinction without a difference here.

Mr. P. Lawrence: That is about it, Mr. Robinson.

But, to answer your question, yes, we would recommend that there be more education with regard to the problems of not attending to security, and that there be a much more free opportunity for security equipment to be available at different levels. After all, security, as we have said, is directly related to time and expense, and there are definite reasons for considering different information at different levels of security.

We would recommend that this be attended by the committee and especially that, as the central user of security in Canada, the federal government should also look into its own use and definition of security.

[Traduction]

M. P. Lawrence: Un des problèmes qui existent est l'ensemble des lois, dans le cadre du gouvernement, concernant cette permission que l'on donne au sein des ministères, afin qu'on puisse se prévaloir de différents niveaux de protection. Si j'ai bien compris la chose, et je ne suis pas avocat, les conditions actuelles sont telles que, si l'on touche à autre chose qu'une définition très claire de ce qui constitue un renseignement, que ce soit de nature confidentielle, sécuritaire, secrète, privée, tout, sauf un renseignement qui peut être divulgué à tout un chacun, il faut veiller à la sécurité de ces renseignements de la même façon, c'est-à-dire qu'il faut respecter toutes les conditions nationales concernant la sécurité, c'est-à-dire «tempest» et «crypto». Le coût en est prohibitif, c'est très coûteux, il est difficile d'obtenir l'équipement; beaucoup de gens n'en savent d'ailleurs encore rien.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Aujourd'hui, vous avez dit que vous étiez des fournisseurs de matériel de sécurité au gouvernement fédéral. Croyez-vous que nous disposons de mesures de sécurité suffisantes? Devrait-on disposer de plus de ressources en ce domaine? Que devrions-nous faire que nous ne faisons déjà? Enfin, pourriez-vous nous recommander certaines lois que nous pourrions adopter? Ou la loi sur la sécurité, à l'heure actuelle, est-elle satisfaisante?

M. P. Lawrence: Puis-je faire un retour en arrière? Nous n'avons pas dit que nous sommes fournisseurs de matériel de sécurité, monsieur. Il faut définir les termes. Nous fournissons du matériel électronique et du matériel de télécommunication à ceux qui s'occupent de sécurité. Nous fournissons du matériel qui répond aux normes «tempest». Parce qu'il est question de matériel de sécurité, on croit parfois que cela signifie «crypto», ou qu'il s'agit du genre de matériel qu'il faudrait pour garantir une certaine sécurité. Il y a là certaines définitions qui, à mon avis, intéresseraient ceux qui s'occupent de sécurité en matière de communications, surtout lorsqu'il s'agit de trouver certaines sources et de définir certaines choses. Cependant, nous ne prétendons pas fournir un matériel de sécurité. Nous fournissons un matériel qui servira dans un milieu sûr, protégé par la méthode «tempest». Il me fallait préciser cela.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Peut-être faire une distinction sans différence.

M. P. Lawrence: C'est à peu près cela, monsieur Robinson.

Cependant, pour répondre à votre question, oui, nous recommandons que se fasse l'éducation concernant les problèmes qui surgissent lorsqu'on ne voit pas à la sécurité d'un système, et nous recommandons aussi que le matériel de sécurité soit beaucoup plus facilement disponible pour divers niveaux. Après tout, la sécurité, comme nous l'avons dit, est directement proportionnelle au temps et à l'argent, et il y a des raisons bien précises pour étudier différentes données pour des niveaux différents de sécurité.

Nous recommandons que cela se fasse par votre Comité, et surtout que, en sa qualité de principal intéressé à la sécurité au Canada, le gouvernement fédéral revoie aussi l'usage qu'il fait de la sécurité, ainsi que sa définition.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): What about the security legislation that we have today? Do you feel it is satisfactory?

Mr. P. Lawrence: No; we think it is far too restrictive.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You are shaking your head no, is that right?

Mr. P. Lawrence: I beg your pardon? I am sorry.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You are shaking your head no.

Mr. P. Lawrence: I am shaking my head no. We feel that it is far too restrictive. In the definition, as I explained earlier, if there is anything other than clear information, it has to have a totally black or white condition. There is no grey area for different levels of security.

• 1225

Mr. I. Henderson: Like pregnancy; you are or you are not. It is either fully secure, national security level or clear; there is nothing that can be . . .

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Sometimes these absolutes are not so easy to define; it depends on the criteria.

Mr. I. Henderson: I think perhaps the rules were made prior to the technology advances that have been made in the last five or ten years.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Beatty, you had a question?

Mr. Beatty: I thought I would just ask a question on one final area that was of concern to me. There has been some debate among witnesses before the committee as to the extent of the computer crime. There seems to be an acknowledgment across the board that the potential is there. Now, there is debate over the numbers. From your experience, is there a computer crime problem in Canada today or are we dealing simply with potentiality?

Mr. P. Lawrence: Not being directly involved in computer crime as per the last set of minutes that we have been reading, we too have got a question as to how much crime there is. I think the recommendation made by an earlier group that the committee should look into the study of computer crime is something that we would support as a study. We do not have information with regards to computer crime within the areas that the committee has been addressing, where the chairman was asking whether it is possible to enter into the computer and manipulate the information and therefore change the conditions?

Mr. I. Henderson: We do know of an instance in Ottawa where one computer was being dumped down the line to another computer and there was an intercept van a block and a half away that picked up everything.

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Et qu'en est-il des lois sur la sécurité que nous avons aujourd'hui? Croyez-vous que ce soit satisfaisant?

M. P. Lawrence: Non, nous croyons que toute cette législation est par trop restrictive.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous faites non de la tête, c'est bien cela?

M. P. Lawrence: Je vous demande pardon? Désolé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous faites signe que non de la tête.

M. P. Lawrence: Je fais non de la tête. Nous croyons que c'est beaucoup trop restrictif. Dans la définition, comme je l'expliquais plus tôt, s'il y a autre chose que des données précises, il faut que tout soit expliqué en noir et blanc. Il n'y a pas de zone grise quant aux divers niveaux de sécurité.

M. I. Henderson: C'est comme être enceinte: on l'est ou on ne l'est pas. On a la pleine et entière sécurité, selon les normes de sécurité nationale, ou il n'y a pas de sécurité du tout. Rien ne peut être . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il n'est parfois pas si facile de définir tout absolument; tout dépend des critères.

M. I. Henderson: Je crois que les règlements ont peut-être été édictés avant que l'on ne connaisse les progrès technologiques des cinq ou dix dernières années.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Beatty, vous aviez une question à poser?

M. Beatty: J'ai pensé vous poser une question dans un dernier domaine qui m'intéresse. Certains des témoins divergent d'opinion quant à l'étendue que peut prendre le crime commis grâce aux ordinateurs. Cependant, tous semblent d'accord pour dire que le potentiel existe. Evidemment, il y a un débat sur les chiffres. D'après votre propre expérience, connaissons-nous des problèmes de crimes reliés aux ordinateurs au Canada aujourd'hui, ou traitons-nous ici d'un simple potentiel?

M. P. Lawrence: D'après le dernier compte rendu de votre Comité que nous avons lu, nous ne sommes pas mêlés aussi directement à ce genre de crime et nous nous posons certaines questions, justement, à propos de la quantité. Un groupe précédent a recommandé que le Comité étudie cette question et c'est là une recommandation que nous appuyons. Nous n'avons pas de renseignements à ce sujet dans les domaines auxquels s'intéresse le Comité et je vous donne l'exemple de quand le président voulait savoir s'il est possible d'avoir accès à l'ordinateur et de manipuler les données pour ainsi changer certaines conditions?

M. I. Henderson: Nous sommes au courant d'un incident qui a eu lieu à Ottawa où on soustrayait certains renseignements d'un ordinateur qui communiquait avec un autre et les

[Texte]

Mr. Beatty: Was it a federal government computer?

Mr. I. Henderson: We would rather not say.

Mr. Beatty: The obvious next question is in terms of the federal government's own security standards. Has there been a problem in terms of the confidentiality of information held in federal data bases?

Mr. P. Lawrence: We would be, I think, in a position to say that we have been led to believe there is, but we have not been privy to any particular problem that we have been asked to solve.

Mr. Beatty: Thank you.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You know you have talked about a tempest problem, if I may use your terminology. Is there really at this time a tempest solution? My understanding would be that, first of all, the most common approach would be to contain the emissions from the piece of equipment. Or the other way would be to manufacture equipment that does not have the emissions. Now is this being acted upon?

Mr. P. Lawrence: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Is there such a thing as a tempest solution or security in fact at the present time?

Mr. P. Lawrence: There is such a thing as a solution; by the methods of screening and protecting the transmissions you are unable by tempest specifications to get nearer than, I would say, within a foot before you can detect anything, as opposed to a considerable distance. So the screening process by tempest specifications will provide a form of security.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose your customers or clients basically are government rather than business in general.

Mr. P. Lawrence: At this time, but I think we will see in the next three to four years a tremendous development within the commercial and industrial sector requesting tempest level security, or tempest level protection.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Have you any final words of wisdom that you can leave with the committee? I see our time is up.

Mr. P. Lawrence: I think we definitely have to address this position of the action if you are going back to the definition of a criminal activity or a criminal intent. It is very difficult to come to grips with the information's being read or understood or interpreted in some way as being a criminal offence because we are continually accessing information as human beings without necessarily misusing it.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): From what you are saying then you feel that the

[Traduction]

renseignements étaient interceptés par une camionnette qui se trouvait à un ou deux coins de rue de là.

M. Beatty: Était-ce un ordinateur du gouvernement fédéral?

M. I. Henderson: Nous préférons ne rien dire à ce propos.

M. Beatty: Se pose maintenant, évidemment, la question des normes de sécurité du gouvernement fédéral lui-même. Y a-t-il eu des problèmes pour ce qui est de la confidentialité des renseignements stockés dans les banques de données fédérales?

M. P. Lawrence: Je crois que nous pourrions dire qu'on nous a laissé entendre qu'il y en a, mais on ne nous a jamais demandé de résoudre aucun problème précis à ce propos.

M. Beatty: Merci.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé d'un problème *tempest* si je puis me servir de votre terminologie. Y a-t-il, à l'heure actuelle, vraiment une solution *tempest*? Si j'ai bien compris la chose, tout d'abord, il faudrait empêcher les renseignements de sortir du matériel lui-même. Ou, encore, on pourrait toujours manufacturer du matériel qui n'émet pas le genre de rayon dont vous avez parlé. Fait-on quelque chose à ce sujet?

M. P. Lawrence: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Y a-t-il, à l'heure actuelle, une solution *tempest* ou des méthodes de sécurité?

M. P. Lawrence: Il y a une solution; et grâce aux méthodes de blindage et de protection des transmissions, il est impossible, d'après les normes *tempest*, de s'approcher à moins d'un pied, à mon avis, avant de pouvoir détecter quelque chose par opposition à ce qu'on pourrait appeler une distance considérable. Donc, le procédé de blindage par méthode *tempest* assurera une certaine forme de sécurité.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je suppose que vos clients, fondamentalement, proviennent du gouvernement plutôt que du monde des affaires en général.

M. P. Lawrence: À l'heure actuelle, oui, mais je crois que d'ici trois ou quatre ans, le secteur industriel et commercial aura recours beaucoup plus au niveau de sécurité *tempest*.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Avez-vous quelques dernières pensées à nous laisser? Nous manquons de temps.

M. P. Lawrence: Je crois qu'il nous faut absolument prendre certaines mesures idoines si l'on veut revenir à la définition d'une activité criminelle ou de l'intention criminelle. Il est très difficile d'accuser quelqu'un de crime s'il lit, comprend ou interprète quelque chose, puisque, en tant qu'êtres humains, nous sommes toujours à traiter toutes sortes de données sans nécessairement en abuser.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Donc, on peut en déduire que vous croyez qu'il

[Text]

way to go is for amendments or new sections to the Criminal Code of Canada?

• 1230

Mr. P. Lawrence: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): And that, of course, would be one way of ensuring that since the Criminal Code applies to all provinces of Canada, there would be no question of jurisdiction if the amendments were made to the Criminal Code. And that would be your recommendation?

Mr. P. Lawrence: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you very much for appearing before us today, Mr. Lawrence and Mr. Henderson. You have been very helpful, indeed, and have opened up a complete new vista for us to look at in our subsequent meetings.

The subcommittee will resume consideration of its order of reference on Wednesday, May 11, 1983, at 3.30 p.m. in this same room, at which time Mr. Frank Spitzer, consultant from Toronto, and Mr. Mervin Gentleman, National Research Council, will be before the committee.

The meeting is adjourned.

[Translation]

faudrait apporter des modifications au Code criminel du Canada ou y ajouter de nouveaux articles?

M. P. Lawrence: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Evidemment, puisque le Code criminel s'applique à toutes les provinces du Canada, ce serait-là une façon de s'assurer qu'il n'y aurait pas de remise en question des compétences si ces modifications étaient apportées au Code criminel. Ce serait votre recommandation?

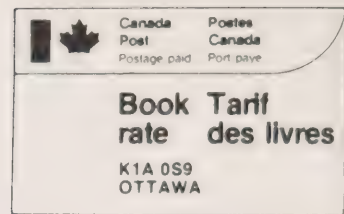
M. P. Lawrence: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci beaucoup d'être venus témoigner ici aujourd'hui, messieurs Lawrence et Henderson. Vous nous avez été très utiles et vous nous avez ouvert de nouveaux horizons que nous explorerons lors de réunions subséquentes.

Le sous-comité reprendra l'étude de son ordre de renvoi, le mercredi 11 mai 1983 à 15h30 dans cette même salle avec M. Frank Spitzer, consultant de Toronto et M. Mervin Gentleman, du Conseil national de la recherche.

La séance est levée.





*If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9*

*En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9*

WITNESSES—TÉMOINS

From Landspan International of Canada Ltd.:

Mr. Peter J. Lawrence, President/Director;

Mr. J. Ian Henderson, Vice-president and General Counsel,
Ottawa, Ontario

De «Landspan International of Canada Ltd.»:

M. Peter J. Lawrence, Président-directeur;

M. J. Ian Henderson, Vice-président et avocat conseil
général, Ottawa, Ontario

HOUSE OF COMMONS

Issue No. 7

Wednesday, May 11, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 7

Le mercredi 11 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

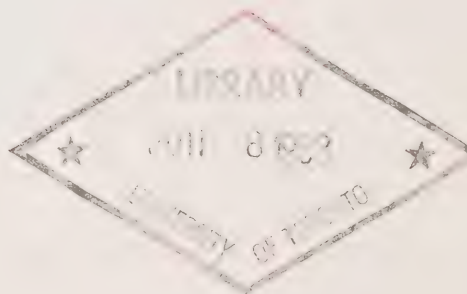
Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, MAY 11, 1983

(9)

[Text]

The Sub-committee on computer crime met this day at 3:46 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: Mr. Morvin Gentleman, National Research Council and Mr. Frank Spitzer, Consultant, Toronto.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements and answered questions.

At 5:33 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 11 MAI 1983

(9)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h46, sous la présidence de M^{me} Céline Hervieux-Payette, présidente.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: M. Morvin Gentleman, Conseil national de la recherche, et M. Frank Spitzer, consultant, Toronto.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations et répondent aux questions.

A 17h33, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Comité

Pierre de Champlain

Clerk of the Committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Wednesday, May 11, 1983

• 1547

Le président: La séance du Sous-comité sur les infractions relatives aux ordinateurs est ouverte.

Cet après-midi, nous entendrons comme témoins M. Frank Spitzer, conseiller, qui vient de Toronto, et M. Morvin Gentleman, du Conseil national de la recherche à Ottawa.

Mr. Gentleman, you are the one starting with your advice and maybe Mr. Spitzer afterwards, and we will be in a position to ask some questions after. So thank you and welcome to our committee.

Mr. Morven Gentleman (National Research Council): Let me introduce my remarks by give you a little background on the context in which I am making them. I am a professor of computer science at the University of Waterloo, and have been for 14 years. I ran one of the computing centres at the University of Waterloo for a period of eight years which has given me experiences as being on the customer side of running a computer service, and I have directed over a period of 11 years a program of producing software which is distributed worldwide and often on a commercial basis, and so I also have experience as a vendor.

I have additional experience that has come up because of the fact that I do consulting and have been asked to provide assistance for people who in some case have had problems relating to computer crime over several years.

I also got a certain amount of notoriety a few years ago over a practice that I instituted at Waterloo. In order to learn something about how hard or easy it was to break computer systems and in order to locate the problems and dangerous places in our computer system, I instituted a policy of offering a pitcher of beer to any student who could find a new way to break the system. Somehow or other that managed to end up getting mentioned in the House and getting in the press, and people got very upset about it. I still think that as a method of finding out where problems are it was extremely effective.

The committee, I gather, has to address a number of questions. First of all, is there a problem associated with computer crime? The immediate answer I would like to give is yes, and I will illustrate that by some examples in a few minutes. In terms of the things you have already heard, I am interested in talking about problems that are associated with the computer as an object of abuse rather than the computer as an instrument.

The second kind of question you are considering, and which I have an immediate answer to, is: Can problems be handled within the framework of current law? My conclusion has been that it does not appear to be the case. I am not a lawyer, obviously; I do not know what can and cannot actually be

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mercredi 11 mai 1983

The Chairman: The Sub-Committee on Computer Related Crime will start its meeting.

This afternoon, our witnesses are Mr. Frank Spitzer, Consultant from Toronto, and Mr. Morvin Gentleman, from the National Research Council

Monsieur Gentleman, c'est vous qui allez commencer et, ensuite, nous écouterons M. Spitzer avant de passer aux questions. Bienvenue parmi nous.

M. Morven Gentleman (Conseil national de recherche): En guise de préambule, permettez-moi de vous décrire le contexte dans lequel je vais vous faire cet exposé. Je suis professeur d'informatique à l'Université de Waterloo depuis 14 ans. Pendant huit ans, j'ai dirigé l'un des centres informatiques de cette université, ce qui ma permis de connaître les problèmes des clients de ce genre de service; de plus, pendant 11 ans, j'ai dirigé un programme de fabrication de logiciel qui est distribué dans le monde entier et même parfois commercialisé, de sorte que j'ai également l'expérience de vendeur.

Par ailleurs, étant donné que je fais de la consultance, j'ai eu l'occasion, depuis plusieurs années, d'aider ceux qui avaient des problèmes dans le domaine des infractions relatives aux ordinateurs.

J'ai également fait parler de moi, il y a quelques années, à cause d'une pratique que j'avais instaurée à l'Université de Waterloo. En effet, afin de connaître davantage les possibilités d'intrusion dans les circuits informatiques, et afin de repérer les éléments vulnérables de ces circuits, j'avais annoncé que j'offrirais une chope de bière à tout étudiant qui me ferait par d'une nouvelle façon de commettre ce genre d'intrusion. D'un façon ou d'une autre, cette pratique a fini par faire parler d'elle à la Chambre et dans les journaux, suscitant de réactions très négatives chez certaines personnes. Pourtant, j suis toujours convaincu que c'était une méthode très efficace pour déceler les problèmes.

À mon avis, le Comité doit trouver une réponse à un certain nombre de questions. Tout d'abord, les infractions relatives aux ordinateurs posent-elles un problème? D'emblée, je dirai oui, et je vous en donnerais des exemples tout à l'heure. Dans le contexte des témoignages que vous avez déjà entendu j'aimerais vous dire que, moi, ce qui me préoccupe, ce sont les problèmes qui sont reliés à l'ordinateur en tant qu'objet d'abus plutôt qu'en tant qu'instrument.

La deuxième question que vous devez examiner, et à laquelle j'ai déjà une réponse, est celle-ci: Ces problèmes peuvent-ils être résolus dans le cadre de la législation actuelle? À mon avis, cela ne semble pas être le cas. Certes, je ne suis pas avocat, et je ne sais donc pas ce qu'on peut et ne peut pas faire

[Texte]

done, but what I do observe is that we do not seem to be getting any help out of the current law.

And the third general question is: What kind of legislation might help?

• 1550

Of course, the useful thing that has been brought forward is the Hon. Perrin Beatty's private member's bill, and I am going to classify that in terms of the things that it does and in terms of something which it does not do by observing that it addresses the problem of theft of computer programs and data, vandalism in the form of alternation damage or destruction of data and software, and the issue of treating computer output as originals for evidence, especially in a case where there is nothing except that.

The item that I would like to talk about that is not treated by that legislation is the question of unauthorized use of computers... well, I will say a bit more about that in a minute.

There are a number of general things that I want to talk about. I guess the first thing I would like to talk in terms of is that whatever appears in the form of legislation there is a very serious problem about enforcement and application. Let me discuss that under a number of headings.

One of the things that is brought up in Bill C-667 is that there is a question of scale in terms of when somebody does something how serious it really is, and there is an attempt in there to make the qualification on scale by distinguishing between calculators, hand-held calculators, and computers. As an expert in the area I have not the faintest idea what the distinction between a calculator and a computer is.

In order to illustrate that, I have brought with me today a computer. This is an extremely powerful computer. It does arithmetic. It does word processing. It allows you to save and retrieve detailed pieces of information in the form of an electronic filing cabinet. It maintains and looks up addresses, providing you with an electronic address book. It will dial your telephone for you so you do not have to remember telephone numbers. If you want to call Larry Smith, you say "Find Larry Smith" and you press the call button and it will dial the telephone for you. It can be used as a terminal to connect to other computers. You can transfer files from other computers into it and then transfer them from it into other computers so you can carry data with you from place to place. You can preserve data in here for months even when it is turned off. It can control peripherals such as printers or bar code readers or tapes. Those are all things you would expect of a computer.

On the other hand, as you can see, it is clearly hand held. It is battery powered. Its normal mode is sitting here turned off. It looks just like a calculator. In fact, I could show you an equivalent thing that looks more like a calculator which is

[Traduction]

sauf cependant, je constate que la législation actuelle ne semble pas nous être d'une grande utilité.

La troisième question générale que vous devez vous poser est la suivante: Quel genre de loi nous serait utile?

Bien sûr, il y a le bill privé qui a été déposé par Perrin Beatty et qui présente déjà une certaine utilité; à ce sujet, permettez-moi de vous expliquer en quoi ce bill est utile et en quoi il ne sert à rien. Ce bill s'attaque au problème du vol de programmes et de données informatiques, au problème de vandalisme, dans la mesure où les données et le logiciel ont été modifiés, endommagés ou détruits, ainsi qu'à la question de savoir si les imprimés d'ordinateurs doivent être considérés comme des originaux pour les besoins de la preuve, surtout lorsqu'il n'y a rien d'autre.

Par contre, ce bill ne parle pas de l'utilisation clandestine des ordinateurs, et c'est ce dont je vais vous entretenir maintenant, ou tout au moins dans quelques instants.

Il y a plusieurs questions générales que j'aimerais aborder avec vous. La première constatation dont j'aimerais vous faire part c'est que, quelle que soit la loi adoptée, son exécution et son application poseront certainement de graves problèmes. Permettez-moi d'en aborder plusieurs aspects.

Dans le Bill C-667, on distingue plusieurs degrés quant à la gravité de l'infraction commise; on essaie également de faire correspondre ces degrés à des instruments différents, c'est-à-dire selon que l'infraction a été commise avec des calculatrices de poche ou des ordinateurs. Je suis pourtant spécialiste dans ce domaine, mais je n'ai pas la moindre idée de la distinction qui existe entre une calculatrice et un ordinateur.

Pour illustrer ce que je viens de vous dire, j'ai apporté avec moi un ordinateur. Il est extrêmement puissant. Il fait des mathématiques, du traitement de texte et il vous permet d'entreposer et de récupérer des données sous la forme d'un classeur électronique. Il peut tenir à jour votre carnet d'adresses, composer vos numéros de téléphone, dont vous avez donc plus besoin de vous souvenir. Ainsi, si vous voulez appeler Larry Smith, il vous suffit de dire à l'ordinateur «Trouve Larry Smith, d'appuyer sur le bouton approprié et l'ordinateur composera le numéro de téléphone pour vous. Il peut également vous servir de terminal de liaison avec d'autres ordinateurs. Ainsi, vous pouvez y entreposer des dossiers provenant d'autres ordinateurs et les transférer ensuite à d'autres ordinateurs, ce qui vous permet de transporter vos données là où vous voulez. Dans cet ordinateur, vous pouvez garder des données pendant des mois, même sans l'utiliser. Il peut contrôler des éléments périphériques, comme les imprimantes, les trieuses/liseuses de code à bâtonnets ou des bandes. Généralement, un ordinateur peut faire tout cela.

Par ailleurs, comme vous pouvez le voir, c'est un ordinateur de poche, qui fonctionne avec des piles. En mode normal, quand il n'est pas en service, il ressemble tout simplement à une calculatrice. En fait, je pourrais vous montrer un appareil semblable qui ressemble encore davantage à une calculatrice et

[Text]

smaller. The only reason this thing is the size it is in order to have the space to have a proper keyboard on it.

I understand that there is a good reason for wanting to make some kind of a distinction based on scale, but that does not seem to me a useful distinction.

Let me talk about a second issue with respect to enforcement and application, and that is the problem of how you know when something is stolen. If you assume that there is a reasonable model of the world that says that software and data are something useful, you have considerable trouble knowing when a break and enter occurred, when something has actually been removed. Let me give you, in fact, three examples in our experience at Waterloo of this happening.

I got a telephone call one day from a manager in a major Canadian company apologizing for the fact that he had discovered that one of his employees, who had been a former student at Waterloo, had stolen a program from us which we sell on a commercial basis and was using it. The manager informed me that having detected that this was happening they were destroying all copies of it and apologized for the incident. We had no way of knowing that in fact a copy had been made, and I do not even know how many months before that incident a copy had been made. It was entirely accidental that we discovered that the phenomenon occurred. That is one sort of example.

• 1555

You could argue that in some sense that was our fault, in not providing proper protection to make sure that the former student, the employee of this company, was unable to access our machine, because he was unable to go through appropriate access controls once he had left; and perhaps it was. But the next incident illustrates that that is not in and of itself the only thing you have to worry about. One of the things that have changed over the years in the computing industry is that it is not true the computer and all of its software and all of its data belong to one person any more.

Another incident occurred some time later, after this first one I have described, where we similarly got informed by a manager in a major, in this case United States, manufacturing company, that a copy of a program that we sell commercially had been illegally, or at least inappropriately, obtained by their employees from a third party's computer system. The third party in fact had the right to have it. We certainly have no way of detecting when a third party's computer system is entered. It might even have been entered in a legitimate manner. But what was not legitimate was removing from the third party's computer system a copy of a program which we had provided to them.

The third incident of not knowing about something being stolen happens to be a case which you have heard about before, the Dalton School incident. In the case of the Dalton School incident a number of machines were attacked—maybe that is

[Translation]

qui est plus petit. La seule raison pour laquelle cet ordinateur a des dimensions aussi grandes, c'est pour l'équiper d'un clavier adéquat.

Je comprends que l'on cherche à faire une distinction de degré en fonction de la gravité de l'infraction, mais à mon avis, celle-ci n'est pas très utile.

Parlons maintenant de l'exécution et de l'application de la loi qui pourra être adoptée dans ce domaine. Le problème qui se pose alors consiste à déterminer comment on s'est rendu compte que quelque chose a été volé. Il est en effet très difficile de déterminer à quel moment il y a eu intrusion et à quel moment on a retiré un élément du logiciel ou des données. Permettez-moi de vous en donner trois exemples que j'ai eu l'occasion de rencontrer à Waterloo.

Un jour, j'ai reçu un coup de téléphone d'un directeur d'une grande société canadienne, s'excusant d'avoir découvert que l'un de ses employés, qui était un ancien étudiant de l'Université de Waterloo, nous avait volé un programme que nous vendions dans le commerce. De plus, il utilisait ce programme. Le directeur m'a dit qu'après avoir découvert l'affaire, ils avaient détruit toutes les copies qui en avaient été faites, et il s'excusait encore de l'accident. Nous n'avions aucun moyen de savoir qu'une copie avait été faite et je ne sais même pas combien de mois auparavant cette infraction avait été perpétrée. C'est donc par pur accident que nous avons découvert le pot aux roses. Voilà un exemple.

Certes, vous me direz que c'était notre faute, dans un certain sens, puisque nous n'avions pas pris les précautions nécessaires pour que cet ancien étudiant, devenu employé de cette société, n'ait plus accès à notre ordinateur étant donné que, une fois qu'il était parti, il ne disposait plus des contrôles d'accès appropriés. Nous étions donc peut-être fautifs. Cependant, l'incident suivant montre bien que cela n'est pas, en soi, tout ce qui doit nous inquiéter. L'industrie de l'informatique a beaucoup évolué depuis quelques années et il est faux de dire que l'ordinateur et son logiciel, ainsi que toutes les données qu'ils contiennent, appartiennent à une seule personne. Cela n'est plus vrai.

Un autre incident s'est donc produit après celui que je viens de vous décrire, où le directeur d'une grande société de fabrication américaine nous a avertis qu'une copie d'un programme que nous vendions dans le commerce avait été illégalement, ou tout au moins clandestinement, obtenue par certains de ces employés à partir de l'ordinateur d'un tiers. Ce tiers avait en fait le droit de posséder ce programme. Il nous est absolument impossible de savoir à quel moment l'ordinateur d'une tierce personne utilise ce programme. Il se peut même que cette utilisation ait été légitime. Toutefois, ce qui ne l'était pas, c'était de faire, à partir de l'ordinateur de cette tierce partie, une copie d'un programme que nous lui avions fourni.

Le troisième exemple de vol s'étant produit à l'insu de la victime est un cas dont vous avez déjà entendu parler, puisqu'il s'agit de l'affaire de l'école Dalton. Dans ce cas-là, un certain nombre de machines ont été attaquées, c'est peut-être le terme

[Texte]

the right phrase—by these students, and in some cases the machines were actually penetrated, because the people who ran the systems did not take what are considered in the industry to be standard methods of protecting the data by requiring passwords to be provided before you could access something.

In the case of Waterloo we did, so the attempted attack was rejected, and we did not even know the whole thing had happened until such time as the people who were complaining reported that here was a list of all the machines that had been attacked and we discovered we were on the list.

Not in the sense of attacks but in the sense of people attempting to use a machine, attempting to gain access to a machine, and through a typing error or through the use of a wrong telephone number or something, ending up trying to get into a machine which they are not authorized to, or appear not to be authorized to, and the attempt is rejected: that happens so often it is simply not worth bothering to keep track of such attempts.

I have said there is a problem of defining a computer. I have said there is a problem of knowing about something being stolen. There is another very serious problem, which is how you identify a stolen object. When something physical is stolen, you can usually recognize what it looks like when you find it is there. In the case of programs and data, one of the things that are different—not only can you make a copy without damaging the original, but it is extremely easy to make radical changes in the copy you have made so that the copy no longer in any simple way looks like the original. Functionally it is equivalent to the original.

Those changes are something so easy to make that in some cases they are things that we do all the time just in the form of using the program. Consequently the transliterated thing is completely unrecognizable. We have had experience with this as a disguise by students we have caught cheating. Actually, it does not happen very often, because most students who are dumb enough to cheat are dumb enough not to take any kind of precautions either—or maybe that is a statement that says the ones we catch have that property. But some of them, in fact, go to a little bit of effort, and for example, will change all the names in the program, will change the spacing in the program, can make changes so that a person looking at the listing of the two pieces of program would never recognize them as being related.

• 1600

I suppose one of the questions you might ask is: If somebody does that, is it the same program? That has been a matter of some concern in the computing industry. One of the things that has been drawn up repeatedly as an example of the fact that you should be able to say those are the same thing is the way British copyright law treats the transposition of music, which has much the same properties, where transposition does not change it from being the same thing.

[Traduction]

qu'il faut employer, par des étudiants et, dans certains cas, il y a eu intrusion véritable car les responsables des circuits informatiques n'avaient pas adopté les normes de protection aujourd'hui requises dans l'industrie et n'exigeaient pas l'emploi de mots de passe pour avoir accès à leurs circuits.

A Waterloo, par contre, nous avons adopté de telles normes et c'est pour cela que la tentative d'attaque a été rejetée. Nous ne savions même pas qu'il y avait eu vol, jusqu'au moment où ceux qui faisaient une plainte ont produit une liste de toutes les machines qui avaient été attaquées, et nous avons constaté que nous figurerions sur cette liste.

Quand je parle d'attaque, ce n'est pas au sens propre, mais c'est plutôt la tentative d'utiliser une machine, d'essayer d'avoir accès à cette machine, et, grâce à une erreur de frappe ou en employant un mauvais numéro de téléphone, finir par avoir accès à une machine de façon clandestine, ou tout au moins en apparence, et que la tentative est rejetée: cela se produit tellement souvent que ce n'est pas la peine d'essayer de contrôler ce genre d'incident.

J'ai dit tout à l'heure qu'il était difficile de définir ce qu'est un ordinateur. J'ai dit également qu'il est difficile de savoir à quel moment un vol est commis. L'autre problème très important consiste maintenant à identifier l'objet volé. Quand un objet concret est volé, vous pouvez généralement le reconnaître lorsque vous le retrouvez par la suite. Dans le cas des programmes et des données informatiques, non seulement pouvez-vous en faire une copie sans abîmer l'original, mais il est aussi extrêmement facile de modifier radicalement la copie que vous avez faites de sorte qu'elle ne ressemble absolument plus à l'original. Sur le plan fonctionnel, c'est toutefois l'équivalent de l'original.

Il est très facile de faire ces changements, à tel point que, dans certains cas, il y a des choses que nous faisons tout le temps simplement dans le cadre de l'utilisation du programme. En conséquence, la chose modifiée est complètement méconnaissable. Nous avons eu un cas de ce genre avec des étudiants que nous avons surpris en train de modifier des données. En fait, cela ne se produit pas très souvent, car la plupart des étudiants qui font la bêtise de resquiller font également la bêtise de ne pas prendre les précautions nécessaires... Enfin, c'est peut-être ceux que l'on prend qui ont cet attribut! Mais certains d'entre eux se donnent du mal et changeront par exemple tous les noms du programme, ainsi que l'espacement, de telle sorte qu'une personne qui examinerait le listing de deux parties du programme ne saurait jamais qu'il existe un lien entre elles.

Vous pourriez peut-être vous demander si dans un cas pareil, il s'agit du même programme? C'est la question que l'on s'est posée dans l'industrie des ordinateurs. Pour montrer qu'il s'agit bien du même programme, on a souvent invoqué à l'appui l'exemple du droit d'auteur dans la loi britannique, en matière de transposition de musique dont les propriétés sont analogues, car la transposition n'empêche pas la musique de rester la même.

[Text]

Just to show you I am not concerning myself here with a hypothetical matter, some years ago I was brought in as an expert in a case that occurred in Halifax, where an employee of company A left and went to work for company B; and magically, company B started to advertise that they were marketing something which was exactly equivalent to a product company A had had. People got enough concerned about the fact that it was exactly equivalent to suspect that actually the program had been carried across; and I was brought in to identify that this had actually happened and show that it was really the same program.

That turned out to have a lot of very interesting aspects to it. The actual program was stored in the computer of the third company; and when we went in with the search warrant and the sheriff to execute this thing, the third company went into a complete tizzy about what was going to happen about their other customers who were on-line in the computer at the time. How could you seize this computer and investigate what was in it? What were their rights and responsibilities with respect to their customer, which happened to be company B, the one that was under suspicion?

Then we discovered that, in fact, company B had got wind of the fact that something was up and so had destroyed the data which was on the computer, but we were able to find records of back-ups that had been taken. So we had properties of this data that we could compare with properties of the original data. It happened that there was something of the order of 300 files. We knew what the file names were; we knew what the sizes of the files were, and they matched identically the ones from the original company. I suppose that illustrates that it is not just students who, when they cheat, are sometimes too stupid to do anything about it.

I suppose another relevant thing to mention about this example is that it illustrates what happens with respect to a lot of computer crime. It never actually appears in the form of court records, because nobody really is sure you could take something like that to court. But when you have a clear enough set of evidence, people tend to back down, and so the whole matter ended up being settled out of court.

There is one final aspect I want to point out about this question of identifying a stolen object. Particularly in the case of distributed products for micro-computers, there has been a serious attempt to try to be able to know when something is stolen and be able to identify a stolen object by restricting the amount of copying that can be done, the number of copies that can be made of a piece of computer software or a set of computer data. Unfortunately, in a pragmatic sense, that does not work very well. It is technically much too easy to make copies of things. But if you back off a minute and say what would you like to have be the case, you discover that restricting the number of copies is something that is not very meaningful to talk about, because in the ordinary course of doing a computation, many copies get made of a program, of data. Some of them are identical copies that you make for back-up in case anything happens to the recording media.

[Translation]

Pour vous montrer qu'il ne s'agit pas d'une question purement théorique, je peux vous rapporter un fait: Il y a quelques années, on m'a fait venir comme expert pour une affaire qui s'était produite à Halifax, et qui concernait un employé qui avait quitté une société A et avait été embauché par une société B. Cette dernière s'est mise tout à coup à faire de la publicité pour un produit qui était exactement semblable à l'un des produits qu'avait eu la société A, au point qu'on se mit à soupçonner que le programme avait été effectivement transféré. On fit appel à moi pour découvrir si tel avait été le cas, et pour prouver qu'il s'agissait du même programme.

Il s'avéra que l'affaire présentait des caractéristiques très intéressantes. Le programme réel était emmagasiné dans l'ordinateur d'une troisième société et lorsque nous nous présentâmes avec le mandat de perquisition et le shérif pour son exécution, la tierce compagnie se mit à s'affoler à l'idée de ce qui allait arriver aux autres clients qui étaient connectés à ce moment-là. Comment s'emparer de cet ordinateur et examiner ce qu'il contenait? Quels étaient les droits et responsabilités de la tierce société envers leur client, qui était en l'occurrence la société B, à savoir le suspect?

Nous découvrîmes alors qu'en réalité, la société B avait eu vent qu'il se passait quelque chose, et avait ainsi détruit les données en ordinateur, mais nous sommes parvenus à trouver des enregistrements de support de sorte que nous connaissions des éléments de ces données aux fins de comparaison avec les données originales. Il existait environ 300 fichiers, nous connaissions leurs noms, ainsi que leur taille et ils correspondaient exactement à ceux de la société originale. Ceci vous prouve qu'il n'y a pas que les étudiants qui, quand ils trichent, ne sont pas assez intelligents pour bien tricher.

Cet exemple montre également bien ce qui se produit dans beaucoup d'infractions relatives aux ordinateurs. De nombreux cas ne sont jamais renvoyés devant les tribunaux, parce que nul n'est certain que l'on puisse tenter des poursuites dans des cas de ce genre. Mais lorsque vous avez des preuves suffisamment flagrantes, les gens ont tendance à s'incliner, et toute l'affaire fut réglée à l'amiable.

Il y a un dernier aspect que je voudrais mettre en relief sur cette question d'identification d'un objet volé. On a vraiment essayé—en particulier dans le cas de produits diffusés pour microordinateurs—d'essayer de savoir s'il s'agit de produits volés et de les identifier en limitant le nombre de copies qu'il est possible de faire du logiciel d'un ordinateur, ou d'un jeu de données d'ordinateur. Dans la pratique, malheureusement, cela ne marche pas très bien. Il est beaucoup trop facile, au plan technique, de faire des copies. Mais si vous réfléchissez une minute et vous demandez ce qu'il faut en ce cas, vous constatez qu'il ne sert pas à grand chose de limiter le nombre de copies parce qu'en faisant un calcul, il est habituel de faire plusieurs copies d'un programme, plusieurs copies des données. Certaines d'entre-elles sont les copies identiques que vous faites pour les archives de réserve, au cas où il y aurait une panne d'enregistrement.

[Texte]

[Traduction]

• 1605

Some are merely a comment that the computer data or the program moves from place to place—it moves from a disc, for instance, into main memory before it goes into execution. So you end up with multiple copies simply because that is the way computation is done, and if you decide to put legal restrictions on how many copies somebody can make, you want to be very careful that you do not end up producing something that is nonsense because copies are required in order to actually be able to accomplish anything.

Those are problems under the general question of enforcement and application of any legislative rules produced.

Let me talk about a slightly different thing for a minute. I would like to talk a little bit about the illegitimate use of computers, something which is clearly anti-social and probably ought to be illegal but which is not discussed in Bill C-667. I would like to start talking about this by saying that if you look at some of the supporting literature, one of the reasons this is not discussed there is the belief that processors are becoming cheap enough that eventually the problem of stealing computer time will not exist. I would support that. I think it is unlikely that in the long run processor time will be very important.

However, that is not the only computer resource that exists and some of the other computer resources, far from getting cheaper are getting more expensive. Storage: the ability to store some information on a computer and retrieve it later, especially storing something where you did not have the right to store it, and where you retrieve it at some point of your convenience, the cost of that is also going down. But because of the fact that it may very well have a long-term effect, and because it does consume resources that someone else might want to use, it can represent a serious problem.

Incidentally, in the university environment that is often a far more serious problem than stealing computer cycles. The computer cycles will go away if they are not used, but the storage will not go away if it is not used.

Communications: I am going to come back to this because the last thing I am going to talk about is computers as a communications device. But I want to point out that all modern computers are only interesting if they can communicate with other things—even this unit is interesting only because it is capable of being plugged into other word processors or other computers. Communications costs are not necessarily cheap. It is in fact the case that theft of telecommunications is a criminal offence, but what is a problem for people running computers is not simply the telecommunications part, it is the whole systems part, the fact that you expected to have communication amongst many parts of the computer system, and that consuming some of that communication represents consuming a real resource and inflicts inconvenience or damage on the computer system over and above the inconvenience or damage that is caused by so many

A vrai dire, les données informatiques ou le programme se déplacent d'un endroit à l'autre—du disque par exemple à la mémoire principale avant l'exécution. Vous vous retrouvez donc avec de multiples copies simplement à cause de la façon dont les calculs sont effectués, et si vous décidez d'assujettir à des restrictions légales le nombre de copies que quelqu'un peut fabriquer, il vous faudra faire bien attention de ne pas vous retrouver en train d'exiger quelque chose qui na aucun sens parce qu'il faut des copies afin de vraiment pouvoir exécuter quoi que ce soit.

Voilà des problèmes qui touchent à la question générale de la surveillance et de l'application de toute règle législative.

Permettez-moi de parler d'un aspect légèrement différent pendant un instant, soit de l'utilisation illégitime des ordinateurs, utilisation clairement anti-sociale et qui devrait probablement être illégale mais dont il n'est pas question dans le bill C-667. J'aimerais commencer par en parler en disant que si vous regardez une certaine documentation, s'il n'en est pas question, c'est qu'on croit que les programmes généraux deviendront assez modiques pour que le problème du vol de temps informatique finisse par ne plus exister. Je suis moi-même de cet avis. Je crois qu'il est fort peu probable qu'à long terme, le temps des programmes généraux soit très important.

Toutefois, ce n'est pas là la seule ressource informatique qui existe et certaines des autres, au lieu de devenir moins coûteuses deviendront beaucoup plus chères. L'entreposage: La capacité d'entreposer certaines données dans un ordinateur pour y accéder plus tard, surtout lorsqu'il s'agit d'entreposer des données sans y avoir droit, pour les récupérer à un moment approprié, voilà quelque chose dont le coût diminuera également. Mais à cause de l'effet à long terme d'une telle procédure, et parce que l'on consomme ainsi les ressources que quelqu'un d'autre pourrait vouloir utiliser, cela peut représenter un grave problème.

En passant, en milieu universitaire, c'est souvent un problème beaucoup plus grave que le vol de cycles informatiques. Les cycles informatiques disparaîtront s'ils ne sont pas utilisés, alors que l'entreposage ne s'évaporerait pas, faute d'usage.

Les communications: J'y reviendrai, car le dernier sujet que j'aborderai, ce sont les ordinateurs comme moyen de communications. Toutefois, je tiens à souligner que tous les ordinateurs modernes ne sont intéressants que s'ils peuvent communiquer avec autre chose—même cet appareil n'est intéressant que parce qu'il peut être branché sur d'autres appareils de traitement de mots ou d'autres ordinateurs. Les coûts de communications ne sont pas nécessairement modiques. C'est un fait que le vol de télécommunications est une infraction criminelle, néanmoins le problème pour ceux qui utilisent des ordinateurs ne se situe pas uniquement au niveau des télécommunications, mais plutôt de l'ensemble des systèmes, et du fait que l'on peut s'attendre à voir de nombreuses composantes d'un système d'ordinateur communiquer entre elles et que par conséquent, si on consomme une partie de ces communications, on consomme une ressource réelle et on inflige un inconvénient

[Text]

seconds of telecommunication having been absorbed. I will come back to a further comment about that in a few minutes.

Another problem with illegitimate use is that programs and data can be illegitimately used. Now, this turns out to be a different thing from what we had talked about as being covered in Bill C-667 because I am not suggesting that you necessarily want to take away the program, or that you do any damage to the program. But a program represents an embodiment of knowledge, and if that is specialized technical knowledge then just running the program, just using it, can produce results that are of considerable commercial value. So the illegitimate running of the program may be worth considerably more than the raw cost of the computer cycles, which is what we used to worry about in days past when we worried about theft of computer time.

• 1610

Similarly, if you have valuable data, the oil companies' logs, for instance, of test shots, it is not so much that you might want to steal the entire data... that would represent a problem—but if you ran a program that used the data and derived from it where you should go to find the next oil well... The commercial value is in using it; it is not necessarily in the original data itself, you would not necessarily have extracted the original data itself, it is this derivative stuff that represents the fact that you have been—well, antisocial.

Those are some general comments about the illegitimate use of computers. I might just say, in passing, what I am sure you have heard before: Everybody who runs a computer centre ends up having experiences with people who, in an anti-social manner, decide to make illegitimate use of the machines. Waterloo has certainly had cases similar to the famous University of Alberta case. They have been detected in strange ways: somebody's happening to notice a student carrying commercial things with him that indicated clearly that he was using the university-provided computer time in order to run a business and, when he was interrogated, he agreed that that was true; students who, in a spirit of frustration, went and damaged other peoples' data sets by logging on through terminals and we then were able to identify, by accident, which terminal a student was using and therefore go and find the people and approach them.

The situation, over the years, has been that our university has quite frequently threatened to take such students, or such employees, to court. The threat has turned out to be effective enough that we have never pursued the actual question of what would happen. I think we all believe that, if we actually did it, it would all fall apart. As long as the threat works, that has not been something we have had to pursue.

I might just observe that if you recognize that the illegitimate use of programs is probably something you want to prevent, an artefact of that is to arrange that illegitimate access to computers is covered, because to get in to use a computer the first thing you have to get past is what is called

[Translation]

ou des dommages au système d'ordinateur, ce qui est plus grave que d'absorber quelques secondes de temps de télécommunications. J'y reviendrai dans quelques minutes.

Un autre problème associé à l'utilisation illégitime c'est le fait que l'on peut utiliser le logiciel et les données de façon illégitime. C'est tout à fait différent de ce que nous discutons lorsque nous avons parlé du bill C-667, car ici il ne s'agit pas nécessairement de prendre le programme, ou de l'endommager. Toutefois, un programme représente des connaissances, et si ces connaissances sont d'une nature technique spécialisée, le simple fait de faire tourner le programme, de l'utiliser, peut produire des résultats d'une valeur commerciale considérable. Ainsi, l'utilisation illégitime d'un programme peut valoir considérablement plus que le coût brut de cycles informatiques, ce dont on avait l'habitude de se préoccuper, à l'époque, lorsque nous nous inquiétions du vol de temps informatique.

De la même façon, si vous avez des données de valeur, par exemple les journaux de sociétés de pétrole par exemple, les journaux des prélèvements, ce n'est pas que vous voudrez peut-être voler toutes les données, cela pourrait représenter un problème, mais si vous faites tourner le programme qui utilise ces données pour trouver le prochain puits de pétrole... La valeur commerciale réside dans le fait de s'en servir et non pas nécessairement dans les données originales; il n'est pas nécessaire de prendre les données originales, c'est ce qui en découle qui fait que vous avez été, eh bien antisocial.

Voilà quelques remarques générales sur l'utilisation illégitime des ordinateurs. Je pourrais peut-être ajouter, en passant, quelque chose que vous avez entendu auparavant, j'en suis persuadé: toute personne qui administre un centre d'informatique finit par identifier des gens qui, d'une manière antisociale, décident de faire une utilisation illégitime de ces appareils. Waterloo a certainement vu des cas semblables à la fameuse affaire de l'Université de l'Alberta. On s'en est rendu compte de façon étrange: quelqu'un a remarqué un étudiant transportant des documents commerciaux ce qui montrait clairement qu'il se servait du temps informatique fourni par l'université afin d'administrer une entreprise, et lorsqu'il a été interrogé, il l'a reconnu; des étudiants qui, par frustration, endommagent les données d'autres utilisateurs en accédant au système par terminal et c'est par accident, que nous avons pu identifier quel terminal utilisait l'étudiant et donc aller le trouver et lui en parler.

La situation, avec les années, c'est que notre université a fréquemment menacé de tels étudiants ou de tels employés de les poursuivre devant les tribunaux. La menace s'est avérée suffisamment efficace et nous n'avons pas eu à nous interroger sur ce qui se passerait. Je suis d'avis que nous croyons tous que si nous le faisons, tout s'écroulerait. Aussi longtemps que fonctionnent les menaces, nous n'avons pas eu à y donner suite.

Permettez-moi de vous faire remarquer que si vous admettez qu'il faut probablement empêcher l'utilisation illégitime des programmes, il faut en contrepartie prendre des dispositions pour que l'accès illégitime aux ordinateurs soit également prévu, car pour utiliser un ordinateur, il faut en premier lieu

[Texte]

the log-in software, software that recognizes that this access attempt is legal. Of course, if using a program illegitimately is illegal, then using the program that lets you in, when you are not supposed to get in, is illegal.

The final set of points that I would like to comment on concerns the final outcome of the Alberta precedent and a very serious implication that that has for the industry. The Appeal court and the Supreme Court both ended up deciding that a computer is not a piece of telecommunications equipment, and that is simply wrong. That is an obsolete view of how computers are used.

Many computers, in fact, exist solely because they are communications devices. Many computer manufacturers view the product they are producing entirely as a communications device. A communications device can be based on a relatively short time frame. One of the services that is particularly popular on modern computers is what is called electronic mail, where two people communicate by one of them entering into a computer a message that he wants to have reach the other person. That message may just stay in the computer that it was written into or it may be moved from that computer to some other computer, but eventually the recipient, when he accesses his computer, discovers that there is a message waiting for him. That kind of service, as I said, which is called electronic mail, is extremely valuable. In the long run it will be a communications mechanism as significant in society as the post office and the telephone are today and it is definitely a form of telecommunications. There are commercial companies who install computers solely for the purpose of doing that.

• 1615

They are, in fact, general computers and, indeed, that particular kind of service is available on essentially every time-sharing system manufactured by anybody today. So here we have a service that on a very short timeframe—typically the time it takes for you to leave a message and for the recipient to pick it up—can be as short as milliseconds if both of you happen to be using the computer at the moment, or can be measured over weeks if it happens that you do not both use it at the same time. That service is something one wants to be able to get and one wants to be able to cover.

Another kind of problem associated with the fact that computers really are communications devices is that a lot of the role of computers is to have data written into them which will be read back by somebody at a later time. That can be and, indeed in the computing industry often is, viewed as communication. The principal thing that you want to do in structuring saving and retrieving data like that is to make the understandability of the information that you saved high for the person who is later going to read it. And a good deal of the computing that you do is not to do arithmetic, but to make things more understandable.

There are two final things I might point out which are problems that occur because of the fact that the computer is, in fact, a communications device, which one might want to think about addressing. One of them is the use of the computer

[Traduction]

contourner le logiciel d'entrée, un logiciel qui reconnaît qu'une tentative d'accès est légale. Evidemment, si l'utilisation illégitime d'un programme est illégale, alors l'utilisation du programme qui vous y donne accès alors que vous n'y avez pas droit est également illégale.

Les derniers points au sujet desquels j'ai des remarques à faire portent sur le résultat final du précédent en Alberta et des très graves répercussions que cela a eu pour l'industrie. La Cour d'appel et la Cour suprême ont toutes deux statué qu'un ordinateur n'est pas une pièce d'équipement de télécommunication ce qui est tout simplement faux. C'est là une opinion dépassée sur la façon d'utiliser les ordinateurs.

En fait, de nombreux ordinateurs n'existent que comme appareils de communication. De nombreux fabricants d'ordinateurs voient leur produit comme uniquement un appareil de communication. Un appareil de communication peut servir pendant assez peu de temps. L'un des services particulièrement populaire des ordinateurs modernes est ce que l'on appelle le courrier électronique, où deux personnes communiquent en inscrivant un message dans l'ordinateur à l'intention de l'autre. Ce message peut rester dans l'ordinateur d'entrée ou être acheminé à un autre ordinateur, mais le récipiendaire, lorsqu'il utilisera son ordinateur, finira par découvrir qu'un message l'attend. Ce genre de service, comme je l'ai dit, qu'on appelle le courrier électronique, a beaucoup de valeur. A long terme, ce sera un mécanisme de communication aussi important pour notre société que les postes et le téléphone le sont aujourd'hui et c'est très certainement une forme de télécommunication. Il y a des sociétés commerciales qui installent des ordinateurs uniquement à cette fin.

En fait il s'agit d'ordinateurs généraux et ce service en particulier fait partie de la plupart des systèmes à temps partagé fabriqués aujourd'hui. Il s'agit donc d'un service que l'on peut obtenir dans des délais très brefs, le temps nécessaire pour faire passer un message et qu'il soit reçu. Il se peut qu'il ne s'agisse que de quelques millisecondes si les deux interlocuteurs utilisent l'ordinateur à un moment donné mais il peut s'agir aussi de semaines si les deux interlocuteurs se servent de l'ordinateur au même moment. C'est un service que l'on veut obtenir et que l'on veut pouvoir couvrir.

Il y a un autre problème qui découle du fait que les ordinateurs sont des mécanismes de communication. Un des rôles majeurs des ordinateurs est de pouvoir enregistrer des données écrites qui seront lues par quelqu'un plus tard. On peut donc dire qu'il s'agit de communication et dans l'industrie informatique c'est considéré ainsi. L'élément principal ici dans la structure de la rétention et de l'accès aux données est la compréhension des renseignements que l'on garde à l'intention d'une personne qui s'en servira plus tard. Une grande partie de l'informatisation n'est donc pas arithmétique mais concerne la clarté du message.

Je voudrais signaler deux autres éléments en terminant qui sont des problèmes provenant du fait que l'ordinateur est un mécanisme de communication, et sur lesquels il convient de réfléchir. D'une part, l'utilisation de l'ordinateur menace les

[Text]

to threaten people. In case this strikes you as being an unusual idea, I have already given you a description of the electronic mail mechanism as a communications device; for example, there was an incident that occurred in Kitchener—Waterloo I think about a year ago now—I have forgotten exactly the timeframe—where in fact there was a court case over harassment because of somebody sending . . . well, it happened to be a love triangle situation. Anyway, somebody was sending threatening computer mail messages to people. Once you recognize the computer as a communications system just like all other communications systems, it can have the same kind of abuses as all other communications systems. In fact, it may even have them better in the sense that, for example, spreading false information is particularly easy to do if you have a computer helping you generate it. Those are the points I wanted to make.

The Chairman: Thank you. Maybe you could start, Mr. Spitzer, for 20 minutes and then be asked some questions. Will it take longer than that?

Mr. Frank Spitzer (Consultant, Toronto): I will keep myself to your instructions, Madam Chairman.

The Chairman: I would appreciate it taking maybe 20 minutes so that we will have enough time for some questions afterwards.

Mr. Spitzer: Following the example of Dr. Gentleman, I will qualify my position here. Most of the experience I have gained and the exposure I have had which has led me to be here today, is in trying to enforce a security system of some kind on the students and users of the University of Toronto computing systems. Again, let it not be said that I am any longer with the University of Toronto, however. So it is experience from that.

I will take issue with some of the comments which my colleague here has made and I will agree with many of them. Notably, I would totally endorse the concept that the definition as Mr. Beatty has proposed it of a hand-held device is an unfortunate move. I think, if I may suggest, that we have to be very careful. In my formal brief which I will turn to in a moment, I have drawn the concern of changing ethics and changing morals to people's attention.

I think we have also got to be careful of the fact that the computer has changed its position in our society in a very very few years. Most other technological developments have had to be addressed by the law and by the social values of society, but have typically made their way into society over a period of several generations.

• 1620

What has happened with the computer is that the first computer ever commercially manufactured is not yet 40 years old, yet we are in the position where machines like this are becoming commonplace. Our children already in many cases know more about those machines than we ever will know. They are growing up and becoming experts in those machines before they have the discretion to know what is right and what is wrong.

[Translation]

gens, Au cas où l'idée vous paraît saugrenue, je vous rappelle la description que j'ai faite du courrier électronique en tant que mécanisme de communication. Il y a un an environ, à Kitchener—Waterloo, par exemple, il y a eu un procès où l'on accusait quelqu'un de harcèlement. Il s'agissait d'une histoire amoureuse, l'éternel triangle. Quoi qu'il en soit, quelqu'un envoyait des messages menaçants par courrier informatique. Une fois que l'on admet que l'ordinateur constitue un système de communication comme les autres, on reconnaît qu'on peut en abuser comme des autres. En fait, l'ordinateur est peut-être beaucoup plus sujet à des abus car il permet de diffuser de faux renseignements, ce qui est d'autant plus facile quand c'est l'ordinateur lui-même qui les fabrique. Voilà les deux choses que je voulais signaler.

Le président: Merci. Monsieur Spitzer, vous disposez de 20 minutes et ensuite nous passerons aux questions. Votre exposé sera-t-il plus long que cela?

M. Frank Spitzer (expert-conseil, Toronto): Madame le président, je m'en tiendrai à vos directives.

Le président: Je vous serais reconnaissant de ne prendre que 20 minutes que pour nous puissions poser des questions.

M. Spitzer: À l'instar de M. Gentleman, je voudrais apporter des précisions ici. L'expérience que j'ai acquise, ce qui m'amène ici aujourd'hui, provient du fait que j'ai essayé de concevoir un système de sécurité pour protéger les systèmes informatiques de l'Université de Toronto auxquels ont accès les étudiants et d'autres usagers. Je vous en prie, qu'on ne dise pas que je suis de l'université de Toronto cependant. J'ai travaillé là-bas.

Je voudrais prendre le contre-pied de certaines remarques de mon collègue et abonder dans le même sens que lui à d'autres égards. En effet, je suis d'accord avec lui pour dire que la définition proposée par M. Beatty concernant un mécanisme que l'on peut tenir dans la main n'est pas très heureuse. Je vous exhorte à la prudence ici. Dans mon mémoire, auquel je reviendrai dans un instant, j'ai attiré l'attention sur une éthique et une morale en évolution.

Il faut également bien se rendre compte que l'ordinateur n'a plus la place qu'il avait dans notre société il y a encore quelques années. La plupart des innovations technologiques ont dû faire l'objet de nouvelles lois et de modifications des valeurs sociales mais elles se sont installées dans la société au cours de plusieurs générations.

Par contre, le premier ordinateur fabriqué commercialement n'a pas encore 40 ans et voilà que ces machines sont désormais courantes. Nos enfants dans beaucoup de cas en savent plus long sur ces machines que nous n'en saurons jamais. Au fur et à mesure qu'ils grandissent ils deviennent experts bien avant de savoir distinguer entre le bien et le mal.

[Texte] SPITZER

The point I wish to make is that the law takes some years to evolve, and it is done by a process of which we are a part here today, and which in part, albeit there it is a legislative procedure, is also a procedure of consensus and a procedure of understanding. I am concerned that any legislation that is proposed should not have in it the inevitable time bombs of being outdated before it can be brought to bear on the problems that are facing us today.

We also have to make sure that any law that is brought forward is of a variety which is and will be enforced. Again, we quote from the examples of our environment, and I quote a story where I apprehended an individual who willingly admitted his guilt in interfering with the University of Toronto's computing facilities. We went through a procedure, which I was required to follow, of passing it up to the university president for action, and he basically shelved it for close on a year. I subsequently discovered, while investigating another computer infraction, that this individual had been hired by another department as a staff member responsible for running their computer while they were quite ignorant of the fact that he had signed a statement admitting guilt in having committed a similar crime already.

The other problem is the problem of detection. I am worried a little about the issue of agency enforcement. The problem of detection is an immense one. Again I will use the same example, the Dalton School children, who randomly dialled numbers and ultimately found their way into a variety of computers.

The isolation, as far as we were concerned—as a user site, we in fact do log failed log-ons; and we were able to identify that there was a failed log-on. But then, for the same reasons you quite correctly alluded to, there are failed log-ons regularly, and they attract no attention; nor, I think, are they of concern. The individual who walks down the street and tries car doors and finds most of them closed is not likely to get apprehended by the police, I think, until he finds one open and goes in.

I cannot quite agree with Dr. Foreman's suggestion that the cost of time is irrelevant. I think we are dealing here with the issue of legislation and not with the cost of damages. I think they are two separate issues.

The communications issue he alluded to—I would venture the suggestion that it is even more straightforward; it is a communications device, if you bear in mind that computers are used for paging devices with voice messages today, and voice storage of messages. If anybody is worried that communications means, in the legal sense, human-to-human communications, then those computers very much are fulfilling that role and certainly are in that context communication devices.

I assume everybody has a copy of the brief I presented to the National Consultation on Computer Crime, which took place in Toronto in early March. Basically I tried in that document to raise my concerns throughout this area. I have not tried to provide solutions except in a very limited context.

[Traduction]

Je tiens à dire qu'il faut des années pour préparer des lois, comme en témoigne notre présence ici aujourd'hui, et bien qu'il s'agisse d'un processus législatif, il s'agit également d'un processus de consensus et de compréhension. Il faudrait éviter à tout prix que la loi proposée ne soit désuète avant qu'elle ne serve à régler les problèmes auxquels nous faisons face aujourd'hui.

Il faut nous assurer que toute loi adoptée puisse être appliquée et quelle le soit. Pour citer un exemple précis, je vous rapporterai le cas d'une personne qui a reconnu spontanément qu'elle était coupable d'avoir abusé des installations informatiques de l'Université de Toronto. Il y a eu une procédure, qu'on m'a demandé de suivre, et j'ai saisi le président de l'Université de la question pour qu'il intervienne. Il a laissé le cas de côté pendant un an. Entre temps, alors que je faisais enquête au sujet d'un autre crime informatique, j'ai découvert que cette personne avait été embauchée par un autre département et qu'elle était responsable de l'ordinateur là-bas, ses patrons ignorant qu'il avait signé des aveux reconnaissant qu'il avait déjà commis un crime semblable.

Il y a également un problème de la détection. Je m'inquiète un peu de la question de l'agence qui sera chargée de l'application de la loi. Le problème de la détection est énorme. Je vais vous donner un exemple. Les enfants de l'école Dalton avaient au hasard composé des numéros et étaient parvenus à avoir accès à divers ordinateurs.

Les lieux d'utilisation des ordinateurs sont parfois isolés et il y a parfois des demandes de connexion erronées. On a pu identifier qu'il y en avait eu une pour les mêmes raisons que vous avez signalées à juste titre, il y a constamment des demandes de connexion erronées qui passent inaperçues. Personne ne s'en inquiète, je pense. En effet la personne qui en descendant une rue essaie les portières de toutes les voitures et découvre qu'elles sont toutes fermées à clé ne se fera pas arrêter. Il faut pour cela qu'il en ouvre une et qu'il pénètre dans la voiture.

Je suis tout à fait d'accord avec la proposition de M. Foreman à savoir que le coût du temps est sans importance. Il s'agit ici d'une loi et non pas du coût des dommages. Ce sont deux choses très différentes.

Il a parlé de la question des communications. Je dirais que c'est encore plus simple que cela. L'ordinateur est un mécanisme de communication si on reconnaît que les ordinateurs sont utilisés pour l'enregistrement de la voix. Si quiconque a des doutes sur la signification de communication du point de vue juridique, communication d'un humain à un autre, qu'il se rassure car les ordinateurs sont certainement des mécanismes de communication.

Je suppose que tout le monde a copie du mémoire que j'ai présenté à la consultation nationale sur le crime informatique qui a eu lieu à Toronto au début du mois de mars. Dans ce document j'ai essayé de faire connaître mes préoccupations concernant le sujet. Je n'ai pas essayé d'offrir des solutions sauf de façon très limitée.

[Text]

The University of Toronto is a fairly large data-processing environment, processing both large amounts of its own data, meaning its business affairs data, the same as any corporation; using its machines for teaching a very large number of students—and thank goodness, there are a number of bright, inquisitive, and therefore somewhat destructive students around as well—and lastly, providing some commercial use for companies for whom we have unique facilities and who are anxious to use our facilities for that reason. Thus, I think we encompass all the normal commercially available facilities with access to the machine through what is known as the dial switch network; in other words, through any telephone, through long distance equivalent of that, Datapac, Dataroute, and also through leased lines.

• 1625

The terminology of computer crime and computer abuse of course are terminology dependent, and I think it is clear that they both, in and of themselves, are not reasonable terms. People have preferred to use the term "computer as the object of abuse" or "computers as the victim of abuse". I suggest there is also the accidental issue of liability when a computer malfunctions without human intervention and causes, potentially, damage which may be legally an issue.

The concept of a lock on a door and the analogy between that and security systems which exist is a totally valid one. I think everybody here knows full well that while they have a lock on their door and they may have gone and bought and had installed the best security systems that are available, they full well know that in the hands of a skillful individual the pick is mightier than the lock. Likewise, the best security systems that are available are not immune to penetration by the really competent individual. The U.S. military maintains a group of people on call who are referred to as "Tiger Teams". They have yet failed to crack a computer when challenged to do so. The point I am making is, let nobody say that the owner has in his hands the possibility of preventing the abuse of his computer system by people outside of his organization and therefore it is an internal problem only.

Given the fact there are any number of careful things which can be done, the attacker still ultimately can break through. Just as an example of the extent to which some of our students have gone, we have one of our systems which uses passwords in order to prevent logging-on, of course. Those passwords are encrypted according to a fairly complicated algorithm. One of our students using a machine a little larger than that was able to break the encryption algorithm and subsequently dump into that encryption algorithm the entire Webster's dictionary, compare it against the encrypted password file and obtain a number of passwords which allowed them to sign on and proceed to play havoc with the system.

We found out who it was. Unfortunately, there is no law against doing that. And that is why I am here.

Theft, again on the terminology issue, assumes you have a tangible object which is removed and made unusable to the owner through its absence. In the theft both of software, where

[Translation]

L'Université de Toronto est un endroit où il y a beaucoup de traitements de données. D'une part, l'Université se sert des ordinateurs pour ses propres besoins, ses propres affaires, comme toute autre société. D'autre part, les ordinateurs servent à l'enseignement à l'intention d'un grand nombre d'étudiants. Grâce au ciel, il y a certains étudiants brillants, curieux, mais il y en a d'autres qui sont un peu destructeurs là-bas. En dernier lieu, l'Université offre des services commerciaux à des sociétés car elle dispose d'installations uniques que les sociétés ne demandent pas mieux d'utiliser à cette fin. Ainsi, nous englobons toutes les installations commerciales habituelles en ayant accès à la machine grâce au réseau commuté; autrement dit, les téléphones, les appels interurbains, Datapac, Dataroute et les lignes prises en location.

Les notions de criminalité informatique et de piratage informatique dépendent de la terminologie, bien entendu; ces notions, de toute évidence, ne sont pas exprimées dans des termes raisonnables. On a préféré parler de l'ordinateur comme victime d'abus, par exemple. Du point de vue légal, il faudra peut-être également étudier la question des dommages causés par le mauvais fonctionnement d'un ordinateur sans que l'être humain n'intervienne.

Le concept de la serrure et l'analogie entre la serrure et les mécanismes de sécurité est tout à fait valide. Tout le monde sait très bien que malgré la serrure, malgré le meilleur mécanisme de sécurité qu'on a pu installer, aucun système n'est à l'épreuve des experts. Parallèlement, les meilleurs mécanismes de sécurité possibles ne sont pas à l'épreuve d'une personne très compétente. Aux États-Unis, les militaires font appel à un groupe de personnes connues collectivement sous le nom de *Tiger Teams*. On leur a demandé de percer un code; ces gens n'ont pas pu le faire. Voici à quoi se résume ce que je veux vous dire: personne ne peut dire au propriétaire qu'il peut empêcher les gens de l'extérieur d'abuser de son système informatique et qu'il s'agit donc d'un problème interne seulement.

Malgré toute la prudence possible, au bout du compte, un mercenaire pourra toujours réussir à percer le code. Jusqu'où nos étudiants peuvent-ils aller? Je vais vous en donner un exemple. Nous avons un système qui fait appel à des mots de passe pour faire obstacle aux procédures d'entrée en communication avec le système. Ces mots sont codés grâce à un algorithme assez compliqué. Grâce à une machine un peu plus grande que cela, un de nos étudiants a pu percer le code et, par la suite, y vider tout le contenu du dictionnaire Webster, le comparer aux mots de passe codés et obtenir un certain nombre de mots de passe qui ont permis à nos étudiants d'entrer en contact et de bousiller tout le système.

Nous avons trouvé le coupable. Malheureusement, il n'a enfreint aucune loi en faisant cela. Voilà pourquoi je me trouve devant vous.

Lorsqu'on parle de vol, on suppose qu'il s'agit de subtiliser un objet tangible de sorte que son propriétaire ne peut plus s'en servir. Dans le cas de vol de logiciel, il s'agit de copies de temps

[Texte]

we are talking of copies, or of computer time, where we are talking of the use of computer cycles, theft in that context as defined by the current Criminal Code, as I understand it, is not satisfied.

When I sign on to the computer and I use Mr. Trudeau's account and his password on to somebody's computer, I am impersonating Mr. Trudeau. That might be regarded as impersonation, except that according to my advice with respect to the Criminal Code, that presumes that is a personal representation and not a representation along a telephone communication line communicating in digital format.

The issue of forgery, likewise, depends ultimately on tangibility and falls down in the context of computer. If I modify exam marks or grades, until that certificate is presented there is no crime of forgery. The Criminal Code, as far as I understand, specifically states: the tangible object in which there has been an alteration of a genuine document in some material part. So maybe the issue there is the definition of document. Document has, I think, been legally interpreted to be something I can hold in my hand.

The issue of personation likewise suggests, and I quote: "... everyone who fraudulently personates any person living or dead." Again, it has to be a person.

• 1630

Most computer crime thus falls into what we may loosely define as theft of time, theft of information, modification of data, or on the other hand, interference with the operation of a system, interference with the use by an individual of a computer system—in other words, denying them access to the system—or the use of the computer as an instrument in the perpetration of a criminal offence; for example, code breaking such as I referred to.

I have already alluded to the fact that, in my personal opinion, the reason the problem is as severe as it is because of the explosive rate of technological development, allowing the technology to be in the hands of anybody and everybody at a rate which has been unprecedented. The result, as I say, is that ethics and morals—the understanding of what is right and what is wrong—is not there.

If we talk for a moment, the theft of time I think is well understood. I presume nobody has any problems with that. The theft of information is an extremely difficult one. It can have very direct commercial implications. If you steal a mailing list from a corporation which is in the business of providing mailing lists as part of its business, it has lost the ability to sell that mailing list. Some companies are in the business of customizing mailing lists, and that is their entire business; and instead of a hit rate for marketing purposes of one per thousand, they will up that to 10 per thousand or 100 per thousand. That has a very substantial commercial value.

A lot of people worry about the invasion of privacy. Multiple sales organizations have got to the point where they call sufficient information—sometimes obtained by questionable means, I will add—into such mailing lists as I was referring to.

[Traduction]

d'ordinateur, d'utilisation de cycles informatiques; dans ce contexte, la définition de «vol» du Code criminel actuel, ne suffit pas, si je l'ai bien comprise.

Lorsque j'exécute la procédure d'entrée en communication en utilisant le numéro de compte et le mot de passe de M. Trudeau, je me fais passer pour M. Trudeau. On peut croire que le certificat n'est pas présenté, il n'est pas question de falsification. Si je comprends bien, le Code criminel précise qu'il doit s'agir d'un objet tangible, d'une contrefaçon d'un document véritable. Il faudra donc préciser la définition de document. Selon l'interprétation légale, un document est une pièce que je peux tenir en main.

De même, l'idée de tangibilité intervient également dans la question de falsification qui peut être étudiée sous l'angle informatique. Je peux changer les notes d'examen; du moment que le certificat n'est pas présenté, il n'est pas question de falsification. Si je comprends bien, le Code criminel précise qu'il doit s'agir d'un objet tangible, d'une contrefaçon d'un document véritable. Il faudra donc préciser la définition de document. Selon l'interprétation légale, un document est une pièce que je peux tenir en main.

Quant à l'usurpation d'identité, on est coupable, et je cite: «... quiconque frauduleusement se fait passer pour une personne, vivante ou morte...». Encore une fois, il doit s'agir d'une personne.

La majorité des infractions informatiques se retrouvent dans les catégories suivantes: vol de temps-machine, vol d'information, modification de données, obstacle au bon fonctionnement du système, obstacle à l'utilisation d'un système informatique par une autre personne, autrement dit lui refuser l'accès au système, et enfin utilisation de l'ordinateur pour perpétrer un délit, par exemple, le décriptage d'un code auquel j'ai fait allusion.

J'ai déjà dit que selon moi le problème est devenu pressant à cause de l'explosion informatique, qui met à la portée de tous et chacun la technologie à un taux inégalé. Il en résulte, selon moi, que le code de déontologie et de moralité qui aurait pu s'appliquer n'existe pas.

Pour en revenir aux catégories, on comprend bien, celle du vol de temps-machine. Le vol d'information est une question beaucoup plus délicate. Cela peut avoir des répercussions commerciales directes. Si une liste d'envois d'une société faisant affaires dans la vente des listes d'envois est volée, la société perd la possibilité de vendre cette liste. Certaines entreprises ne font rien d'autre que d'adapter aux besoins particuliers de chacun les listes d'envois; ainsi, les clients dans leur campagne de commercialisation ont des résultats 10 fois ou 100 fois meilleurs. On comprend bien la valeur commerciale de ces listes.

Un grand nombre de personnes s'inquiètent de l'invasion possible de leur vie privée. Les organisations de ventes multiples rassemblent maintenant des informations d'une façon parfois douteuse, et je dois le dire, à même ces listes

[Text]

It seems to me the computer is being used as an instrument of abuse in that case, not as the object of abuse.

The person who signs on to a computer will not necessarily recognize that his files are being used, as you have heard. Worse than that, since he cannot recognize immediately they have been used, he may under certain circumstances also not recognize that they have been modified. I refer to the gentleman who was hired by one of the University of Toronto departments; what he was guilty of doing was tampering with electronic mail, so that people would receive electronic mail purporting to be from another individual, sent at times when those other individuals were nowhere in the country. The result was, of course, that this was not easily detectable. He had managed to do certain things in a relatively sophisticated way. Here you have multiple levels of what I would refer to loosely as computer crime at the same time.

On the issue of software confidentiality, again, you have heard what happened at the University of Waterloo. The issue has been resolved by different people in different ways. Quite common practice from a number of software vendors is to provide what is in the trade known loosely as "a time bomb" in that the date is coded in a fairly sophisticated manner so that the program will cease to function after a certain date, unless the licensee has extended the licence and has been told what modification to make; and these modifications are far from transparent, I will add.

That works to some extent. You can steal the software, but the stealing will only work for a limited period of time and then will cease to function. The danger is that that system is great. What happens if you have a disgruntled employee who leaves the Department of National Defence and plants a time bomb to go off three weeks after he has left in some critical area of software? You do not know when it was planted; nor do you know where to go looking for it, necessarily. I am not about to provide solutions, I hasten to add; these are quite substantial problems.

The individual, I think, as an individual public citizen, must be guaranteed the right to verify what is beginning to be gathered in very large computer data banks, precisely because of the reasons I have been alluding to. Somebody in the department who has a grudge against me can modify the data and yet I cannot see it, I cannot access it, I cannot verify it. We have a very serious responsibility there.

• 1635

There is a famous survey done by Professor Carroll from the University of Western Ontario, I believe, with respect to the ethics of students and computer science. He has determined, which comes back to the statement I have been making, that more and more frequently it has become acceptable for students to rip off the system. Some years ago everybody was law abiding and reasonable. Today it is more than reasonable to have a go and see whether you can get away with it. I think that pervades a lot of my concerns. We also certainly have seen some instances... and I have seen one recently where I apprehended a student and I accused him of abusing one of

[Translation]

d'envois auxquelles je faisais référence. Il me semble qu'ici l'ordinateur sert à perpétrer l'abus et n'en est pas l'objet.

La personne qui a accès à un ordinateur ne se rendra pas nécessairement compte que ses dossiers sont utilisés, comme on vous l'a dit. Pire encore, comme cette personne ne peut se rendre compte immédiatement que ses dossiers ont été utilisés, il est possible que dans certains cas elles ne se rende pas plus compte que les dossiers ont été modifiés. Je pense ici à l'individu qui avait été embauché dans une des facultés de l'Université de Toronto; cette personne a modifié l'acheminement du courrier électronique, si bien que des personnes recevaient du courrier électronique que leur aurait envoyé une autre personne, alors que ceux-ci n'étaient pas au pays. L'infraction n'a pas été facile à découvrir. Cet individu a réussi à faire des choses d'une façon assez complexe. Dans ce cas-ci, nous avions de nombreux types d'infractions informatiques se déroulant en parallèle.

Au sujet de la confidentialité du logiciel, vous avez entendu dire ce qui s'est passé à l'Université de Waterloo. Différentes solutions ont été apportées aux mêmes types de problème. Assez souvent, les vendeurs de logiciels ont recours à ce que l'on appelle dans le métier une «bombe à retardement» en vertu de laquelle une date est codée de façon à ce que le programme cesse de fonctionner après cette date, à moins que le vendeur n'ait autorisé le détenteur du programme à faire les modifications nécessaires; je dois ajouter ici que ces modifications ne sont vraiment pas évidentes.

Cela peut fonctionner pendant un certain temps. On peut voler le logiciel mais celui-ci ne sera utile que pendant une période précise et il tombera en panne ensuite. Cette technique pose de graves dangers. Qu'arrive-t-il si un fonctionnaire du ministère de la Défense nationale introduit une bombe à retardement qui paralysera la machine trois semaines après son départ? On ne sait pas où chercher la «bombe» et on ne sait pas non plus quand elle a été posée. Je dois dire ici que je ne peux pas vous donner de solution car ce sont des problèmes assez graves.

Selon moi, la personne, doit avoir le droit de vérifier les données qui sont recueillies à son égard dans une banque de données informatiques, pour les raisons auxquelles je faisais allusion précédemment. Toute personne du service qui a un dent contre moi peut changer les données sans que je puisse le constater, y avoir accès ou le contrôler. Notre responsabilité est très grande dans ces cas.

Une enquête célèbre a été entreprise par M. Carroll, professeur à l'Université de Western Ontario, je crois, sur l'évolution du sens moral des étudiants en informatique. Ses conclusions entérinent ce que je dis: de plus en plus, les étudiants trouvent qu'il est acceptable de voler le système. Il y a quelques années, tout le monde respectait la loi, tout le monde était raisonnable. Aujourd'hui, il est tout à fait légitime de tenter la chose, de voir s'il est possible de s'en tirer indemne. Je me préoccupe beaucoup de cet aspect de la question. Dernièrement, j'ai arrêté un étudiant et je l'ai accusé d'abus informatiques sur un de nos systèmes à l'Université de

[Texte]

our systems at the University of Toronto. He was, after some considerable questioning, able to satisfy me that he had not done anything knowingly. Some other person, whom we subsequently located and apprehended, had planted in his program area a program which this innocent victim executed when he logged on and caused all sorts of havoc, quite innocently and quite unbeknown to him.

The computer as the instrument of abuse: I presume that most of you are aware of tricks like Trojan horses, which is a modern rendition of the ancient scheme. You place an image before the user which appears to be like a normal terminal session, but everything you type—most specifically, your account and its password—neatly get logged onto the Trojan-horse owner's file and he then has your access code.

I believe our biggest problem in most installations—and this is a point, I think, which is important—does not lie with external individuals. Most abuse of computers originates within the department or within the organization owning and running the computer. Certainly this is borne out by what I have read publicly and what I have experienced in discussions with many people. Almost all concerns ultimately end up because the bank had one employee who was greedy—and note I say the word “employee” quite intentionally—or the company or the university had students. These are people who are intended to be using the machine. They are not people who are intended to be forbidden to use the machine. Let us recognize that. When we think about the law we are dealing with a community offence in most cases.

When we do not deal with a community offence access is in most cases through the use of the telephone system. Here I am treading on thin ice because there is an investigation which is currently still in progress, but it is an investigation which has been made extraordinarily difficult because the access has been via the public telephone network, and while the movies and popular media might make us think that it is very easy to call in the RCMP, the Ontario Provincial Police and heaven knows who else and identify within 30 milliseconds that this call originated from this particular office building at that particular phone, it is not so. International boundaries, provincial boundaries, city boundaries and merely central office to central office within the Bell system make any such tracing formidable.

Basically, Bell's position at present is that if you go within one central office—in other words, if somebody is coming in through the same main exchange you are on—there is a reasonable possibility—and I use the words carefully—that they may within half an hour be able to identify where the call is coming from. If you have prealerted them, then they will do better than that; but if you did not know it was going to happen, then you are in that kind of order of magnitude. They may be able to trace it afterwards, but if you are going out of that central office you may as well give up, and you do not even know whether it is a local or a long distance call at that point. The point that becomes extraordinarily significant when you make that comment is that when we talk about police

[Traduction]

Toronto. Après un interrogatoire prolongé, il a réussi à me convaincre qu'il n'avait rien fait sciemment. Une autre personne que nous avons réussi, par la suite, à repérer et à arrêter, avait réussi à insérer un programme à l'intérieur du programme du premier étudiant; victime innocente, cet étudiant exécutait le programme dès son entrée en contact; ainsi, il bousillait le système de façon tout à fait innocente et à son insu.

L'ordinateur, instrument d'abus: La plupart d'entre vous êtes au courant de procédés tels le cheval de Troie, version 20^{ème} siècle. Il s'agit de placer une image devant l'utilisateur qui semble être une session normale de terminal; toutefois, tous les renseignements que vous inscrivez, notamment votre numéro de compte et le mot de passe, sont inscrits sur le dossier du propriétaire du cheval de Troie qui, dorénavant, possède votre code d'accès.

Dans la plupart des cas, le plus gros problème ne réside pas chez les étrangers. La plupart des abus sont commis à l'intérieur du service ou de la Société qui possède et qui exploite l'ordinateur. Cette idée est corroborée par les renseignements qui ont été publiés et les discussions que j'ai eues avec bon nombre de gens. Au bout du compte, on finit par trouver l'employé (je vous signale que j'ai utilisé le mot employé) cupide, l'employé de la Société ou l'étudiant universitaire. Il s'agit de personnes qui devaient utiliser la machine. Il ne sagissait pas de personnes à qui l'utilisation était défendue. Reconnaissons-le. Sur le plan légal, il s'agit d'un délit communautaire, dans la plupart des cas.

Lorsqu'il ne s'agit pas d'un délit à l'intérieur de la même communauté, les coupables ont la plupart du temps accès au réseau grâce au système téléphonique. Je dois faire preuve de prudence car une enquête est actuellement en cours à ce sujet; les travaux de l'enquête ont été rendus difficiles car l'accès au réseau s'est fait grâce au réseau téléphonique public; même si les films ou les moyens de communication populaire peuvent nous faire croire qu'il est très facile d'appeler la GRC, la police provinciale ou autres et de préciser, dans quelque 30 millisecondes, de quel bureau, quel édifice, quel téléphone provient un appel, il n'en est pas ainsi. C'est tout un travail que de retracer un appel; il faut tenir compte des frontières internationales, provinciales, des limites de la ville et de chaque bureau central du système Bell.

Voici, essentiellement la position actuelle de la Bell à ce sujet: si quelqu'un est en contact avec le même réseau principal que vous, il est assez possible et je dis bien assez possible de pouvoir préciser la provenance de l'appel dans les 30 minutes qui suivent. Si vous avez donné un préavis, il sera possible de le faire en moins de temps; mais s'il s'agit d'un appel auquel vous ne vous attendiez pas, les possibilités sont de cet ordre. Il se peut qu'il soit possible de le retracer, mais si l'appel ne relève plus de ce bureau central, vous faites mieux d'oublier, ne sachant même pas à ce moment-là s'il s'agit d'un appel local ou d'un interurbain. Ce qui devient extrêmement important au sujet de votre commentaire, c'est que lorsque nous parlons d'agences policières... J'en ai eu l'exemple il y a quelques

[Text]

agencies . . . Again, I had an example in recent months where I was approached by one of the police agencies which was extremely interested in an investigation involving the U of T computer facilities. It also involved computing facilities outside of Canada. The problem was computer-to-computer communication such as we have been discussing here.

• 1640

I am simplifying the case in order to make it easy to understand. When you deal with a network situation, it is not possible for the user to immediately recognize where the information is really stored. In other words, if you have what is called a network, an efficient communication between two computers, the user does not know where the data is stored. All the user knows is that this information has been requested to be presented upon his terminal, and there it comes. It may have been obtained from 1,000 miles or 1,000 feet. It does not matter.

I do not know how you are going to deal with the corporation that lets an individual go because that individual has misappropriated computer facilities, and I use the terms loosely, and then as a subsequent employee proceeds to embezzle funds for a second time and a third time, because the cost to the company of publicizing this information is more lost business than the amount of money embezzled.

The Criminal Code, I understand, requires that indictable offences cannot be ignored. There may be some safety in that if the law is properly written.

I made note of a couple of additional comments which may just be interesting. We described the issue of the Dalton school children, and we will come back to them for moment.

The computer installations, where they succeeded in gaining access in Canada, had not taken the necessary precautions, we have said, in terms of providing proper passwords. They had in fact provided some passwords, to my understanding, but had not gone through the rudimentary procedures of changing them, as they should have done.

Passwords typically, in most cases, in most installations, by most employees, are selected to be their names, their children's names, their wives' names, etc., because those are names we can easily remember. They are also typically names which most people who know anything about those individuals will guess rather easily.

From a criminal point of view—and bear in mind that I am not worried about the methodology here . . . I am not sure that makes access, using that password, any more legitimate than the guy who happens to have a key which, when he wiggles it around in the lock, opens the door. He is still guilty of breaking and entering at that point.

The other comment is that I made mention of the difficulty of software distribution by vendors. Vendors, of course, are taking some of this into their own hands by only distributing what is called machine language or object code. They are

[Translation]

mois, lorsqu'une agence de police a communiqué avec moi se disant extrêmement intéressée à une enquête concernant les installations informatisées de l'Université de Toronto. Cela touchait également des installations informatiques à l'extérieur du Canada. Il s'agissait de problèmes de communication entre un ordinateur et un autre, comme celui que nous discutons ici.

Je simplifie ce cas afin qu'il soit plus facile à comprendre. Lorsqu'il est question de réseau, l'utilisateur ne peut pas immédiatement savoir où l'information est vraiment conservée. Autrement dit, si vous avez ce qu'on appelle un réseau, une communication efficace entre deux ordinateurs, l'utilisateur ne sait pas où les données sont conservées. Tout ce qu'il sait, c'est qu'on a demandé que l'information soit présentée à son terminal, et elle se présente. Elle peut venir de 1,000 milles ou de 1,000 pieds plus loin. Cela n'a pas d'importance.

Je ne sais pas ce que vous pouvez faire pour la société qui a laissé partir une personne qui s'était servie des installations informatisées à mauvais escient, et j'emploie ce terme très librement, et dont un employé subséquent détourne des fonds une deuxième fois et une troisième fois, car il en coûte plus cher à la compagnie, si ces renseignements sont publiés, étant donné qu'elle perdra des affaires, que le montant de la somme détournée.

Si j'ai bien compris, le Code criminel exige qu'on n'ignore pas les actes criminels. Si la loi est convenablement libellée, elle peut offrir une certaine sécurité dans ce domaine.

J'ai pris en note quelques remarques additionnelles qui peuvent vous intéresser. Nous avons décrit la situation des enfants de l'école Dalton, et nous y reviendrons un peu plus tard.

Nous avons dit que les services d'ordinateurs, là où ils ont pu s'installer au Canada, n'ont pas pris les précautions nécessaires au sujet des mots de passe appropriés. Ils ont offert des mots de passe, si j'ai bien compris, mais ils n'ont pas suivi la procédure élémentaire de changer ces mots de passe, comme ils auraient dû le faire.

Les mots de passe typiques, dans la plupart des cas, dans la plupart des services, ceux qui sont utilisés par la plupart des employés, sont choisis en fonction de leur nom, du nom de leurs enfants, de leur femme, etc., car il est facile de se souvenir de ces noms. Ce sont habituellement des noms que la plupart des gens devineront aisément s'ils connaissent un petit peu les personnes intéressées.

Du point de vue criminel, et souvenez-vous que je ne me préoccupe pas de la méthodologie ici, en se servant du mot de passe, je ne suis pas certain que cela rend l'accès plus légitime que dans le cas d'une personne qui se sert d'une clé et qui, jouant un peu dans la serrure, arrive à ouvrir une porte. Il est quand même coupable d'entrer avec effraction.

J'ai mentionné la difficulté pour les vendeurs de distribuer le logiciel. Les vendeurs évidemment prennent les décisions de ne distribuer que ce qu'on appelle le langage machine ou le code réel. Ils limitent les renseignements qu'ils distribuent au strict

[Texte]

restricting the amount of information they distribute to an absolute minimum, again as a method of trying to reduce their exposure to abuse and danger.

I have spoken a few minutes longer than you allotted me. My apologies. I have gone fairly quickly over the brief, and I have touched on a number of topics. I hope that I have lent something of use to you.

The Chairman: Thank you. Questions?

Mr. Beatty: Thank you, Madam Chairman. First of all, let me thank our two witnesses who I think have delivered two excellent briefs to us today. It has been extremely helpful to the committee, and we very much appreciate your coming.

One thing I am very pleased about is that I am beginning to find some focus, in terms of the various witnesses we have had coming before the committee, in that certain issues continue to come up, and I think we are getting a better handle on the issue.

Mr. Spitzer, you very honestly said that you were not proposing solutions. Unfortunately, the committee is in the position of having to propose solutions. Much of the testimony we have had before the committee has pointed out problems in my bill, or else problems with the law as it stands today, or problems with technology.

• 1645

All of that has been very helpful, but notwithstanding a natural reluctance I think on both of your parts to get into the aspect of solutions, I hope we can perhaps draw on your advice in this area. Perhaps I could start first with Mr. Gentleman.

You pointed out the difficulty of identifying software that has been stolen. I accept that. But both of you have also given illustrations of cases where indisputably a person was culpable, where he may have even signed a statement saying he was culpable, but where there appears to be a hole in the law as things stand today. Mr. Gentleman, in your judgment, is the fact that it is difficult to prosecute justification in itself for not making something an offence—if it is difficult to detect the crime or it is difficult successfully to prosecute? Or should you in fact close any loophole there is in the law in those cases where in fact you have somebody dead to rights and there is no doubt about it? In addition, is there not a salutary effect the law has for normally law-abiding people who are told that what they would otherwise be doing is wrong and society does not approve?

Mr. Gentleman: No; in fact, I would argue almost exactly the opposite to that. I would say that because it is so hard seriously to identify it, in some sense you have to rely on intimidation. You have to rely on the fact that there is the off chance somebody might get caught, and therefore a certain set of people will give up and not commit this unpleasant act because they might get caught. So I think the fact that it is hard to detect things is all the more reason for saying that we ought to have a more useful legal support than we do now.

[Traduction]

minimum, de nouveau pour ne pas être exposés aux abus et aux dangers.

J'ai parlé un peu plus longuement qu'il ne m'était permis. Je m'en excuse. J'ai revu rapidement le mémoire, pour souligner quelques sujets. J'espère que ce sera utile pour vous.

Le président: Merci. Y a-t-il des questions?

M. Beatty: Merci, madame le président. Premièrement, permettez-moi de remercier nos deux témoins qui nous ont présenté d'excellents mémoires aujourd'hui. Cela a été très utile pour les membres du Comité, et nous apprécions beaucoup leur visite.

Tout d'abord, je suis très heureux parce que je commence à comprendre, après la venue des divers témoins au Comité, car certaines questions reviennent sans cesse, cela nous permet de nous faire une meilleure idée de la question.

Monsieur Spitzer, vous avez déclaré très honnêtement que vous ne proposiez pas de solution. Malheureusement, le Comité doit en proposer. Dans la plupart des témoignages que nous avons entendus au Comité, on a souligné certains problèmes au sein de mon projet de loi, ou des problèmes qui existeraient dans la loi actuellement, ou des problèmes de technologie.

Tout cela est très utile malgré une réticence naturelle de votre part à nous parler de solutions. J'espère néanmoins que nous pourrions profiter de vos conseils dans ce domaine. Je vais commencer par M. Gentleman.

Vous dites qu'il est difficile de déterminer la propriété du logiciel volé. Je comprends. Mais vous avez tous deux donné des exemples de cas où une personne était incontestablement coupable, où elle avait peut-être même signé une déclaration de culpabilité, mais où sont ressorties certaines lacunes de la loi. Monsieur Gentleman, à votre avis, la difficulté de poursuivre peut-elle justifier qu'une telle action ne soit pas reconnue comme une infraction, parce que le crime est difficile à déceler? Ne devrions-nous pas plutôt combler toutes les lacunes de la loi afin que les coupables prouvés soient condamnés? En outre, la loi n'aurait-elle pas un effet salutaire pour ceux qui respectent normalement la loi et qui ne feraient rien de ce que la société jugerait mal?

M. Gentleman: Non; en fait, je suis d'un avis tout à fait contraire. Je crois que, comme il est très difficile de détecter ce genre de crime, il faut avoir recours à l'intimidation. Il faut qu'on sache qu'on peut arriver à attraper le coupable et que, par conséquent, certaines personnes ne commettront pas cette action déplaisante parce qu'elles risqueraient de se faire attraper. Le fait que ce crime soit difficile à dépister, vient renforcer la nécessité d'avoir un cadre juridique beaucoup plus utile que le cadre actuel.

[Text]

I guess the related thing, however, is that I point out the difficulties in finding out that something is stolen or in identifying the stolen object as really having been stolen from such and such a place merely to say that one wants to be careful in the wording of whatever legislation appears so that it is not easy to circumvent. We know that it is easy to make those changes. You want to make sure that if you define what constitutes a stolen object, you do not define it in such a way that a trivial change to it circumvents it.

Let me point out that there is in fact a really serious problem about this already today, because many people in many countries have been trying to protect software by copyright; and copyright is one of the things that happen to be very easy to get around, in many countries, by mechanical translations. It is not true everywhere that copyright covers transliterations of things. It only covers identity; and identity happens to be the easiest thing to get around.

Mr. Beatty: I am wondering whether in your judgment the best place to deal with protection of software, though, is not through copyright legislation; possibly through amendments to the Copyright Act. The government is in the process of reviewing it at the present time. I attempted to provide protection in my bill for computer programs and software. I am increasingly drawn to the belief that perhaps the better location for dealing with that would be the Copyright Act.

Mr. Gentleman: I personally think the way it was done in your bill was better.

Mr. Beatty: I was wiser than I knew.

Mr. Robinson (Etobicoke—Lakeshore): This is where you differ, then, with your colleague.

Mr. Beatty: Did Mr. Switzer indicate that he . . .

Mr. Spitzer: I do not think I made any comment, as a matter of fact.

Mr. Robinson (Etobicoke—Lakeshore): No, you did not. But you did in your paper. On page 6 of your paper, in the middle of the page, you say:

Copyright was developed as a concept in respect of the copying of the written word. This would appear to be a bad basis on which to found "computer law".

Then you go on: "Patenting . . ." and so on.

Mr. Spitzer: Yes. But that is exactly, I think, what—I think we are agreed. What I am saying is that the copyright law as it stands is aimed at the written word and is therefore not a basis for dealing with the protection of software. I think we are in agreement about that.

Mr. Beatty: But it is open to amendment.

Mr. Spitzer: Fine. I would have to consider what the form of the amendment is. But I think the better place is to deal with it in the context of computer theft and computer crime. That is, I think, what I am saying here.

Mr. Robinson (Etobicoke—Lakeshore): Well, you do not really suggest that it is a question of changing the copyright law. You sort of make a bald statement that it is a bad base upon which to start.

[Translation]

Je fais ressortir le mal que l'on peut avoir à découvrir un vol de banque puis à déterminer l'origine d'un objet volé justement pour vous faire comprendre que le libellé de la loi devrait être soigneusement choisi afin qu'il soit très difficile de contourner cette loi. Nous savons qu'il est toujours facile de faire certains petits changements. Il faut donc être certains que la définition d'objets volés par exemple ne puisse pas être contournée grâce à une modification insignifiante.

Cela représente déjà un problème grave puisque des tas de gens, dans bien des pays, essaient de protéger leur logiciel par droit d'auteur. Or, dans la plupart des pays, il est très difficile de passer outre aux règles des droits d'auteur en faisant des «traductions» mécaniques parce que ce n'est pas partout que l'on protège les droits contre les translitérations. On protège seulement l'identité et c'est ce qu'il y a de plus facile à contourner.

M. Beatty: Je me demande si, à votre avis, ce ne serait pas la Loi sur le droit d'auteur qui pourrait assurer la meilleure protection des logiciels? Peut-être pourrions-nous alors y apporter des amendements. Le gouvernement est justement en train de la revoir. J'ai essayé dans mon projet de loi d'assurer une certaine protection aux programmes et aux logiciels. Je crois de plus en plus que ce serait la Loi sur le droit d'auteur qui serait indiquée dans ce cas.

M. Gentleman: Personnellement, je crois que c'est votre projet de loi qui y parvient le mieux.

M. Beatty: J'ai plus de talent que je ne le pensais.

M. Robinson (Etobicoke—Lakeshore): C'est là que vous n'êtes pas du même avis que votre collègue.

M. Beatty: M. Switzer a-t-il dit que . . .

M. Spitzer: Non, je crois ne rien avoir dit là-dessus.

M. Robinson (Etobicoke—Lakeshore): Non, c'est vrai. Mais vous en parlez dans votre mémoire. A peu près au milieu de la page 7, vous dites:

Ainsi, le concept du droit d'auteur se rapporte à la copie de documents écrits; il ne semble donc pas souhaitable comme fondement du «droit informatique».

Et vous poursuivez: «pour ce qui est des brevets . . . etc.

M. Spitzer: En effet, mais je crois que nous sommes d'accord. Moi, je dis que la Loi sur le droit d'auteur, dans son libellé actuel, vise les documents écrits et ne peut donc pas être invoquée pour protéger les logiciels. Je crois que nous nous entendons tous là-dessus.

M. Beatty: Mais elle pourrait être modifiée.

M. Spitzer: Très bien. Mais alors il faudrait que je voie l'amendement. Je crois que la meilleure loi serait celle traitant de vol informatique et de crime informatique. C'est ma théorie.

M. Robinson (Etobicoke—Lakeshore): Mais vous ne proposez pas d'amender la Loi sur le droit d'auteur. Vous affirmez péremptoirement que cette loi serait un mauvais fondement.

[Texte]

• 1650

Mr. Spitzer: Yes, I am saying that the copyright law, per se, is probably not the best way of going.

Mr. Robinson (Etobicoke—Lakeshore): So what do you suggest instead?

Mr. Beatty: He is suggesting writing it into a computer bill, similar to what I did.

Mr. Spitzer: That is right. I am sorry; I think we are in agreement.

Mr. Beatty: No, but I am tending to move away from it, thinking that . . . One of the difficulties, which both of you put your fingers on and both of you seized, for example, was on the definition in my bill of "computer", which did not include calculators and other hand-held devices. The reason why it did not include them was a very practical one: If you leave your calculator on your desk and I go and balance my cheque book with it, I do not think I have committed all that serious an offence. It is not the same thing as breaking into the main-frame in the University of Toronto. I am not sure that we wanted to make it an offence for me to borrow your pocket calculator from the desk.

You correctly point out, both of you—and I think Mr. Gentleman was alluding probably to the Sharp or Radio Shack pocket computer, which is considerably smaller than the model he has there—where the distinction between a programmable calculator and a hand-held computer becomes almost beyond comprehension. I accept that. The difficulty, I suppose, with getting into legislation that is highly complex is that you would find that witnesses coming before the committee, or the Department of Justice or others, would argue that because of its very complexity there are all sorts of reasons not to act . . . or not to act now, or to act in a different way. But the purport of both of your testimonies today was that some action is needed, although there is not a consensus as to what the nature of that action is.

I am increasingly beginning to believe that perhaps we should look at software protection as being related to copyright and perhaps deal with other matters related to evaluation of information—whether or not information is property, as such, and so on. One of the reasons for setting that aside would be to have a bill that was much simpler and was capable of enactment speedily. Perhaps we should go in the direction of a crime similar to computer trespass or data trespass, unauthorized access to computer facilities. I am wondering whether I could have your comments on that. I gather from testimony by Professor Flaherty, of the University of Western Ontario, that there is a provision similar to that in the Swedish data protection law. The advantage that I can see is, first of all, simplicity and, secondly, it helps to prevent incongruities between the treatment of manually stored information and the treatment of electronically stored information. If we say that we will suddenly treat information as property if it is stored in a computer but not if it is stored in a filing cabinet, we get into an incongruity based simply on the method of storage, rather than on the nature of the information itself.

[Traduction]

M. Spitzer: Je dis effectivement que la Loi sur le droit d'auteur en soi n'est probablement pas le meilleur moyen.

M. Robinson (Etobicoke—Lakeshore): Que proposez-vous à la place?

M. Beatty: Il suggère la rédaction d'un projet de loi concernant les ordinateurs, comme ce que j'ai fait.

M. Spitzer: En effet. Je suis désolé, mais je crois que nous sommes d'accord.

M. Beatty: Non, car j'ai tendance à m'éloigner de cette idée. L'un des problèmes sur lequel vous avez tous les deux mis le doigt, c'est la définition d'ordinateur dans mon projet de loi qui ne comprend pas les calculatrices et autres machines de poche. Je ne l'ai pas fait pour une raison bien pratique: si vous laissez votre calculatrice sur votre bureau et que je m'en sers pour calculer le solde de mon compte-chèques, je ne crois pas avoir commis un grand crime. Ce n'est pas comme si j'avais accès au gros ordinateur de l'Université de Toronto. Je ne suis pas certain de vouloir considérer comme un crime le fait d'emprunter votre calculatrice de poche qui traîne sur votre bureau.

M. Gentleman a fait allusion à l'ordinateur de poche fabriqué par Sharp ou Radio Shack, lequel est beaucoup plus petit que le modèle qu'il a avec lui, et vous avez tous les deux dit avec raison que la distinction entre une calculatrice programmable et un ordinateur de poche est extrêmement difficile à faire. Je suis d'accord. Le problème, si on en parle dans la loi, est fort complexe car certains témoins, comme le ministère de la Justice et d'autres encore, viendront prétendre qu'à cause de sa complexité même, il y a toutes sortes de raisons pour vouloir s'abstenir d'agir tout de suite ou de cette façon. Néanmoins, la conclusion de vos deux témoignages, c'est qu'il faut agir, même si l'on n'arrive pas à s'entendre comment.

Je crois de plus en plus que nous devrions songer à protéger les logiciels par le biais des droits d'auteur et traiter ailleurs des autres problèmes comme l'évaluation de l'information, sa définition comme bien, etc. Cela permettrait d'avoir un projet de loi beaucoup plus simple qui serait adopté plus rapidement. On pourrait choisir d'en faire un crime comme l'accès sans autorisation aux ordinateurs ou aux données. Je voudrais savoir ce que vous pensez de cela. D'après le témoignage du professeur Flaherty de l'Université Western Ontario, il existerait une disposition semblable dans la loi protégeant les données en Suède. L'avantage à mon sens, c'est d'abord la simplicité, et ensuite la possibilité d'empêcher que l'information emmagasinée manuellement d'une part et électroniquement d'autre part ne soit traitée différemment. S'il faut que nous nous mettions tout d'un coup à traiter l'information comme un bien lorsqu'elle est emmagasinée dans un ordinateur mais pas lorsqu'elle l'est dans un classeur, on se retrouve avec une distinction fondée simplement sur le mode d'entreposage et non sur la nature de l'information elle-même.

[Text]

Mr. Gentleman: I think one of the reasons why I find that I would prefer to have something in the form of the bill that you suggested, instead of using the copyright mechanism, refers to the difficulty about identifying copies. The wording you used left clear what the idea was, that unauthorized "making copies of software or data should be illegal". The trouble with putting it in the copyright law is that you then have to figure out what constitutes something that is a copy. It seems to me that the exact questions of under what circumstances you are allowed to make copies, what transliterations are allowed that represent a copy of the same thing and what ones represent something new and different, are much more serious issues in terms of copyright. In terms of a separate law, the simple intent behind the law is, I think, easier to understand.

Mr. Beatty: Could I just get some clarification? I hate to attack my own bill, there is a feeling of paternity here that makes it difficult, but does not the same problem exist in either case? You have to establish that, in fact, there is something contained in the machine that has been copied—whether you establish it through copyright legislation or through my bill.

• 1655

Mr. Gentleman: Sure.

Mr. Beatty: For example, assume you had a word processing program in the computer. I was entitled to use the computer. I was entitled to even use the program, but I perhaps was not entitled to copy the program. You would have difficulty in establishing that I, in fact, copied your program and did not reconstruct it, working back from the way in which the program itself worked. The same would apply whether we operated under copyright legislation or under my bill, would it not? By making modifications to your program that I was copying, it might be possible to frustrate either my bill or the copyright law.

Mr. Gentleman: I believe all of that is true. I just think the machinery that exists in the rest of the copyright bill complicates the issue in an unnecessary way. If I were to take a trivial example of making a copy, suppose I have a document, in fact, stored in this, which is of value so that one would not want to have it copied; and indeed, one might want to press charges against someone who made a copy of it in an unauthorized manner. I transfer that document between this room in Ottawa and a computer somewhere else; we will say, just for the sake of argument, the University of Waterloo. In doing that, that document passes across telecommunications lines and through intermediate computers that are there for the purpose of storing and forwarding the packets of information as they are being processed. It is, in fact, the case that Bell Canada will have instantaneously copies of that program, just because I cannot move it from here to there without doing that. I do not want to get into a situation where I have to distinguish between that kind of copy, which is going to get made whether or not Bell Canada has any rights to access the program, and a kind of copy where, in fact, somebody really swiped it when they should not have.

[Translation]

M. Gentleman: Je préférerais qu'il y ait un projet de loi semblable au vôtre plutôt que d'avoir recours au droit d'auteur, à cause de la difficulté à identifier les copies comme telles. Votre libellé donne l'impression très nette que toute copie de logiciel ou de données, faite sans autorisation, serait illégale. Le problème de la Loi sur le droit d'auteur, c'est qu'il faut alors définir ce qu'est une copie. Je crois que les questions de savoir dans quelles circonstances vous êtes autorisé à faire des copies, quelles transliterations sont autorisées, ce qui constitue une copie identique et une copie différente, posent des problèmes beaucoup plus graves pour les droits d'auteur. Si c'était une loi distincte, l'esprit de la loi serait beaucoup plus facile à saisir.

M. Beatty: Je voudrais avoir des précisions. Je m'en veux de critiquer mon propre projet de loi, mais le même problème ne se pose-t-il pas dans les deux cas? Ne faut-il pas trouver qu'il y a dans la machine quelque chose qui a été copié, qu'il s'agisse de la Loi sur le droit d'auteur ou de mon projet de loi?

M. Gentleman: Certainement.

M. Beatty: Par exemple, disons qu'il y ait dans un ordinateur un programme de traitement de mots. J'ai l'autorisation de me servir de l'ordinateur et même du programme. Je n'ai toutefois peut-être pas l'autorisation de copier le programme. Vous auriez du mal à prouver que j'ai copié votre programme, car j'ai pu le reconstruire à partir de la façon dont le programme fonctionne. La même chose pourrait se produire, que ce soit dans le cadre de la Loi sur le droit d'auteur ou de mon projet de loi, n'est-ce pas? En modifiant votre programme que j'ai copié, je peux déjouer à la fois mon projet de loi et la Loi sur le droit d'auteur.

M. Gentleman: Je crois que vous avez parfaitement raison. Je crois néanmoins que les mécanismes prévus dans la Loi sur le droit d'auteur compliquent inutilement les problèmes. Si je prends l'exemple banal de la copie toute simple d'un document de valeur dans la mémoire ici, je pourrais tenir à ce qu'il ne soit pas copié. Je pourrais même porter des accusations contre celui qui voudrait en faire une copie sans autorisation. Si je transfère ce document de la pièce ici à Ottawa à un ordinateur qui se trouve ailleurs, disons à l'Université de Waterloo, le document circule alors sur les lignes de télécommunications et passe par des ordinateurs de relais qui servent à emmagasiner et à acheminer l'information traitée. De cette façon, Bell Canada obtiendra instantanément copie du programme, tout simplement parce que je ne peux pas l'envoyer là-bas sans passer par ces autres ordinateurs. Je ne veux pas être obligé de faire la distinction entre ce genre de copie, qui sera faite que Bell Canada ait un droit d'accès au programme ou non, et cet autre genre de copie faite par quelqu'un qui n'aurait vraiment pas dû le faire.

[*Texte*]

Mr. Beatty: Potentially, the courts would have to deal with the same problem, whether in the context of my bill or under copyright legislation. In other words . . .

Mr. Gentleman: Yes, although . . .

Mr. Beatty: —is it appropriate that Bell should have made whatever copy there was, or should there have been a copy stored in the memory of the computer or . . . ?

Mr. Gentleman: I agree, and I guess what I am saying is that I think, if you put it in the context of the copyright legislation, you have to put in all kinds of qualifiers to get rid of the extraneous information and the extraneous rules that appear in the Copyright Act. I prefer the element of vagueness that is present by putting it in all by itself.

Mr. Robinson (Etobicoke—Lakeshore): As a follow-up, just on that point, I wonder . . . You have talked previously about the Criminal Code and knowingly doing something. Here you are saying Bell Canada, in effect, knows they are getting all this information, but it is a question of intent.

Mr. Gentleman: Absolutely.

Mr. Robinson (Etobicoke—Lakeshore): Is that not the distinction?

Mr. Gentleman: Yes.

Mr. Robinson (Etobicoke—Lakeshore): The “knowingly” would not apply in the Criminal Code in a situation like this, but it would be only the word “intent”.

Mr. Gentleman: That is right.

Mr. Beatty: Mr. Spitzer could perhaps elaborate on his feeling on the issue of data trespass or computer trespass.

Mr. Spitzer: Willingly. I would like to get back actually to the . . . You made a couple of comments that I do not think you responded to on the issue of why a calculator, not a computer list.

It seems to me the Criminal Code—and heaven forbid, I am not a lawyer—basically says, if I remove a book from your desk, that is an offence if I do not have your permission. Nobody will press criminal charges, because I believe in order to be an indictable offence it has to reach a minimum of \$200; there is a dollar figure associated with it. I would have thought the same kind of mechanism could be used to deal with the issue of the hand-held computer/calculator versus the big machine, by dealing with the issue of the dollar value which is involved in the transaction.

Mr. Beatty: The dollar value to whom? How do you judge?

Mr. Spitzer: To the injured party.

Mr. Beatty: To the injured party.

Mr. Spitzer: Yes.

Mr. Beatty: Dollar value in terms of foregone income or in terms of . . .

[*Traduction*]

M. Beatty: Théoriquement, les tribunaux feraient face au même problème, qu'on invoque mon projet de loi ou la Loi sur le droit d'auteur. Autrement dit . . .

M. Gentleman: Oui, quoique . . .

M. Beatty: . . . est-il normal que Bell ait fait une copie, ou devrait-il y avoir une copie dans la mémoire de l'ordinateur ou . . .

M. Gentleman: C'est vrai, mais je crois que si l'on fait appel à la Loi sur le droit d'auteur, il faudra ajouter toutes sortes de qualificatifs afin de ne pas être touchés par les règles peu pertinentes qu'on y trouve. Je préférerais une loi distincte afin qu'on puisse rester dans le vague un peu.

M. Robinson (Etobicoke—Lakeshore): À ce propos, je me demande . . . Vous avez parlé un peu plus tôt du Code criminel et de l'intention de faire quelque chose. Vous dites maintenant que Bell Canada sait qu'elle obtient toute cette information, mais que c'est une question d'intention.

M. Gentleman: Certainement.

M. Robinson (Etobicoke—Lakeshore): N'est-ce pas la distinction justement?

M. Gentleman: En effet.

M. Robinson (Etobicoke—Lakeshore): Pour le Code criminel, le «sciemment» ne serait pas important, il faudrait qu'il y ait intention.

M. Gentleman: C'est exact.

M. Beatty: Monsieur Spitzer pourrait peut-être nous parler plus longuement de ce qu'il pense des accès non autorisés aux données et aux ordinateurs.

M. Spitzer: Bien volontiers. Je voudrais en fait revenir à . . . Vous avez fait quelques observations sur la raison pour laquelle les calculatrices ne seraient pas comprises dans la définition d'ordinateur et c'est resté sans réponse.

Il me semble que le Code criminel—et Dieu sait que je ne suis pas avocat—prévoit que si je prends un livre sur votre bureau, je commets un crime si je n'ai pas obtenu d'abord votre permission. Personne n'intentara des poursuites pénales parce que, pour cela, il faut qu'il y ait un montant d'au moins \$200 en cause. Il me semble qu'on pourrait utiliser la même chose pour faire la distinction entre les calculatrices et ordinateurs de poche et les grosses machines; on pourrait leur attacher une valeur monétaire.

M. Beatty: Mais la valeur monétaire pour qui? En vertu de quels critères?

M. Spitzer: Pour la partie lésée.

M. Beatty: Pour la partie lésée.

M. Spitzer: Oui.

M. Beatty: La valeur monétaire pour ce qui est du manque à gagner ou . . .

[Text]

Mr. Spitzer: No, that is the basis of the Criminal Code at the present moment; and there are enough lawyers around the table. They can guide me on whether or not I am talking through the back of my head, but...

Mr. Robinson (Etobicoke—Lakeshore): I think you are.

Mr. Beatty: In terms of foregone income or in terms of the cost of compilation of the material.

Mr. Spitzer: I know, if you want to press criminal charges, one of the first questions the police will ask you is: What was the value of the loss? The determination of whether it is an indictable offence or not is measured in terms of that declared loss.

• 1700

Mr. Robinson (Etobicoke—Lakeshore): Not necessarily. You are getting yourself into deeper water all the time.

Mr. Spitzer: It could be used as a mechanism for providing that definition rather than for dealing with a hand-held calculator, which I think is going to be a very dangerous one—certainly, as we move into the future. That is the point I am trying to make.

Mr. Beatty: I can certainly accept your criticism of the hand-held calculator.

Mr. Spitzer: No, I am trying to provide a solution. I am endeavouring to help, and your colleague there tells me that I am muddying the waters and treading on very thin ice.

Mr. Beatty: I have always found it easier not being a lawyer; it is far less confusing.

Mr. Spitzer: The other issue which I totally agree with you on really relates to the issue that information is information. One thing which came out at the consultations in Toronto, and which I assume would have been documented somewhere by the Department of Justice, was a very nice definition of information and of knowledge in this context.

I do not know whether you gentlemen remember; I specifically recollect that it was C.C. Gotlieb who, in fact, enunciated it and, therefore, information is quite independent of the medium and the form which it takes, and must so be in terms of what we are discussing here.

Mr. Beatty: Professor, can you elaborate on the differentiation between information and knowledge?

Mr. Spitzer: Yes. I am just trying to think of the definition we evolved, because we spent a long time discussing it. Do you have it there, gentlemen? It was the distillation of much work, so I would hate to misquote it.

Mr. Beatty: Was it, in itself, a work of art which might be copyrightable?

Mr. Spitzer: Yes. I did not quote it.

Mr. Beatty: Light knowledge is ephemeral, and transitory and easily lost.

Mr. Spitzer: Yes. I do recollect that the final one was "wisdom", and wisdom is what you get when you are old.

[Translation]

M. Spitzer: Non, c'est le fondement du Code criminel à l'heure actuelle, mais il n'y a pas suffisamment d'avocats ici. Ils pourraient me dire si je m'abuse ou non...

M. Robinson (Etobicoke—Lakeshore): Je crois que oui.

M. Beatty: Par rapport au manque à gagner ou par rapport au coût de compilation du matériel.

M. Spitzer: Je sais que la première question que les policiers vous posent quand vous voulez porter plainte, c'est quelle était la valeur du bien perdu? Et c'est cette valeur qui fait qu'un acte criminel a été commis ou non.

M. Robinson (Etobicoke—Lakeshore): Pas nécessairement. Vous vous enfoncez de plus en plus.

M. Spitzer: On pourrait se servir d'une formule semblable pour régler le cas des calculatrices de poche au lieu de se servir d'une définition car cela pourrait être très risqué, surtout avec ce que nous réserve l'avenir. Voilà ce que j'essaie de vous faire comprendre.

M. Beatty: Je comprends votre critique à propos des calculatrices de poche.

M. Spitzer: Non, j'essaie de proposer une solution. J'essaie de vous aider et votre collègue n'arrête pas de me dire que j'embrouille les choses et je m'aventure en terrain glissant.

M. Beatty: J'ai toujours trouvé cela plus facile de ne pas être avocat, c'est bien moins mêlant.

M. Spitzer: Je suis également d'accord avec vous à propos du fait que l'information, c'est de l'information. Ce qui est ressorti des consultations tenues à Toronto, et qui a dû être mentionné quelque part par le ministère de la Justice, c'est une très belle définition de l'information et de la connaissance dans ce contexte.

Je ne sais pas si vous vous en souvenez. Je me souviens que c'est C.C. Gotlieb qui l'a formulée. Par conséquent, l'information est tout à fait à part de l'appareil et de la forme qu'on lui donne, et il doit en être ainsi aux fins de notre discussion.

M. Beatty: Professeur, pouvez-vous en dire plus long sur la différence entre l'information et la connaissance?

M. Spitzer: Oui. J'essaie de me souvenir de la définition que nous avons formulée car nous avons passé beaucoup de temps à en discuter. L'avez-vous ici messieurs? C'était l'essence d'un long travail et je m'en voudrais de ne pas la citer convenablement.

M. Beatty: Était-ce en soi une oeuvre d'art pouvant donner un droit d'auteur?

M. Spitzer: Oui. Je ne l'ai pas citée.

M. Beatty: La connaissance superficielle est éphémère, transitoire et vite oubliée.

M. Spitzer: Oui. Je me souviens que la définition se terminait par «sagesse» et «la sagesse vient avec la vieillesse».

[Texte]

Mr. Beatty: Perhaps we could come back to that.

Mr. Robinson (Etobicoke—Lakeshore): You have been telling us it is the young with these computers!

Mr. Spitzer: I did not say they are wise. No, I did not say they are wise. I said they have a lot of information. There is a difference. Here, we have found what we were looking for. Thank you. Information is data used for decision-making; knowledge is information in which the decision is defined.

Mr. Beatty: I will take that back and muse on it for a while.

Mr. Spitzer: Certainly. I mean any one-sentence, glib definition is open to criticism, but it was an attempt at least to define our terminology here. We have gone a long way from your question, I think, at this point.

Mr. Beatty: Can we go back to data trespass and the virtue, or lack of it, of having something that is very simple and which is not technology-dependent. You set two criteria: first, the law must not be obsolete at the time it is passed; second, it must be enforceable. It seems to me that the simpler it is, the less likely it is to become obsolete and the more enforceable it is likely to be.

Mr. Spitzer: I concur totally.

Mr. Beatty: Could you comment on whether the approach of data trespass or something similar to that—computer trespass, unauthorized access or unauthorized use of computer equipment—would be efficacious?

Mr. Spitzer: Yes. And again I will go back to the discussions we had in Toronto, because there was a distillation of much thinking. There was total consensus certainly amongst the people I spoke with that the moment you executed a single cycle upon a machine without authority, that constituted trespass, and that unauthorized use in that context should be regarded as an offence. Again, one presumably would wish to distinguish in the enforcement phase between what represents merely a minor trespass and a substantial trespass.

Mr. Beatty: Yes, and one can differentiate, too, just as you can with physical trespass. It may be totally appropriate for you to be on the grounds of the University of Toronto under some circumstances during the day in some portions, but you may stray beyond your area into areas where you do not belong, or at the wrong time, and become guilty of trespass.

Mr. Spitzer: That is right; but nonetheless, the university is the body which establishes that, not the law. In the context you have just stated, trespass is defined as "inappropriate place at an inappropriate time".

• 1705

Mr. Beatty: Yes.

Mr. Spitzer: And the university establishes, in your example, what is appropriate.

Mr. Beatty: But it seems to me that the analogy then could even be carried over to time sharing on computers. It may be

[Traduction]

M. Beatty: Nous pourrions peut-être y revenir plus tard.

M. Robinson (Etobicoke—Lakeshore): Vous n'arrêtez pas de nous dire que le problème avec les ordinateurs, ce sont les jeunes!

M. Spitzer: Je n'ai pas dit qu'ils étaient sages. J'ai dit qu'ils avaient beaucoup d'informations. Voilà la différence. Voilà, nous avons trouvé ce que nous cherchions. Merci. L'information c'est une donnée utilisée afin de prendre une décision; la connaissance c'est l'information dans laquelle on définit la décision.

M. Beatty: Je vais la noter et j'y réfléchirai.

M. Spitzer: Certainement. N'importe quelle définition peut être critiquée. Au moins celle-ci tentait de définir notre terminologie. Je crois que nous nous sommes beaucoup éloignés de votre question.

M. Beatty: Pourrions-nous donc en revenir aux accès non autorisés aux données et aux avantages d'avoir quelque chose de très simple qui ne dépende pas de la technologie? Vous avez défini deux critères: premièrement la loi ne doit pas être déjà surannée au moment de son adoption; et deuxièmement, elle doit être applicable. J'ai l'impression que plus la loi sera simple, plus tard elle deviendra désuète et plus elle sera facile à appliquer.

M. Spitzer: Je suis parfaitement d'accord.

M. Beatty: Pourriez-vous me dire si la création d'un crime pour accès non autorisé à des données ou à un ordinateur serait utile?

M. Spitzer: Oui. J'en reviens à nouveau aux discussions que nous avons eues à Toronto, car vous avez là l'essence d'une grande réflexion. Tous les gens avec lesquels j'ai discuté s'entendaient pour dire que dès que vous exécutez un cycle simple sur une machine sans autorisation, vous êtes coupable d'intrusion et un tel accès sans autorisation doit être considéré comme un acte criminel. À l'étape judiciaire, je présume qu'on pourrait faire la distinction entre une intrusion sans grande conséquence et une intrusion aux conséquences graves.

M. Beatty: Oui, il est certainement possible de faire une telle distinction tout comme l'intrusion physique. Vous pouvez être tout à fait admis à l'université de Toronto dans certaines circonstances, dans certains locaux et à certaines heures du jour, mais si vous allez dans d'autres locaux ou si vous vous y trouvez à une heure indue, vous devenez coupable d'intrusion.

M. Spitzer: Vous avez raison. Néanmoins, c'est l'université qui décide de cela et non pas la loi. Dans l'exemple que vous venez de donner, l'intrusion est définie comme le fait d'être au mauvais endroit au mauvais moment.

M. Beatty: Oui.

M. Spitzer: Et dans votre exemple, l'université établit ce qui est approprié.

M. Beatty: Il me semble alors toutefois que l'on pourrait même pousser l'analogie au partage du temps d'ordinateurs.

[Text]

appropriate for you to use a computer for a certain purpose, but when you get beyond that purpose and to other areas of the memory and so on you may be in areas which are unauthorized and where you do not belong.

Mr. Spitzer: I concur totally. I was going to—but I did not wish to because I did not want to talk any longer—deal with an example which my colleague here gave, and that refers to the issue of logging on. I think he made a statement that you can in fact prevent misuse by preventing the log-on in the first place. But in fact certain users may have authority to log on and do certain things but not have the authority to access other information on the same machine.

Mr. Beatty: I think the point is well taken. In any case, the difficulty that I had . . . I accepted at the time Mr. Gentleman had said it that if you can prevent unauthorized access and unauthorized use of the software you can prevent unauthorized use of the hardware, in essence.

Mr. Spitzer: Correct.

Mr. Beatty: But the difficulty is that we get into this area of information again, and information as property, and we raise issues that go well beyond computerization. They go well into the whole concept of information under the law and what control we have over information. The difficulty that keeps being raised is when in the context of trying to do something about computer crime we create special offences which would exist for computers which would not exist with information contained in a manual form. This is why, it seems to me, the best approach may be to keep it simple and go to something like data trespass and then look for other means of dealing with, first of all, the question of protection of software per se. Secondly, Professor Flaherty quite properly pointed out that we, as citizens or as individuals on whom information is stored, may have a right to expect that data security standards of those institutions storing information should be sufficiently high to protect our information. But that is perhaps an issue that can be better dealt with in the context of privacy legislation. I believe you alluded to it as well, Mr. Spitzer, that in some time we must have access to information about ourselves that institutions hold. But the same applies for manually held employee records, for example, and there is no distinction in kind between computer-stored data and manually stored data.

Perhaps that is an issue to be left for another day, and there are various others, but if we could get at the unauthorized access to a computer we at least close off that final loophole, and in any of the instances that you gentlemen have cited where you have had somebody dead to rights who had committed something that you thought was wrong there was at least some charge that could be laid.

Could I ask just two other questions—and I apologize to my colleagues for being lengthy here but . . . First is mandatory reporting. Mr. Spitzer pointed out that with indictable offences you are required to report. But what if it was not an

[Translation]

Peut-être est-il normal que vous utilisiez un ordinateur à certaines fins mais ensuite, si vous accédez à d'autres domaines de la mémoire, etc, vous risquez d'accéder à des domaines non autorisés qui ne vous regardent pas.

M. Spitzer: Je suis tout à fait d'accord. Je ne voulais pas vous prendre plus de temps, mais j'avais justement eu l'intention de revenir sur un exemple qu'a donné mon collègue à propos du problème de l'entrée en communication. Il a je crois dit que l'on pouvait éviter le piratage en empêchant l'entrée en communication. En fait, certains usagers peuvent avoir le droit d'entrée en communication et de faire un certain nombre de choses sans avoir droit d'accéder à d'autres informations contenues dans la même machine.

M. Beatty: C'est certainement tout à fait vrai. De toute façon, la difficulté . . . M. Gentleman avait dit que si l'on pouvait interdire l'accès non autorisé et l'utilisation non autorisée du logiciel, on pouvait essentiellement interdire l'utilisation non autorisée du matériel.

M. Spitzer: En effet.

M. Beatty: La difficulté est que nous nous retrouvons devant cette question de l'information comme propriété qui pose des problèmes qui vont bien au-delà de l'informatisation. On aborde alors tout le concept de l'information et du contrôle que nous avons sur l'information. La difficulté à laquelle on revient toujours est que lorsqu'on essaie de faire quelque chose en matière de criminalité informatique, on crée des infractions spéciales qui existeraient pour les ordinateurs et qui n'existeraient pas si l'information était consignée manuellement. C'est pourquoi il me semble que le meilleur moyen est peut-être de simplifier les choses et d'envisager par exemple de défendre l'accès à certaines données pour trouver ensuite d'autres moyens de protéger tout d'abord le logiciel lui-même. Deuxièmement, le professeur Flaherty a très justement signalé que nous, citoyens ou individus sur lesquels on compile des informations, avons peut-être le droit de nous attendre à ce que des normes sur l'imperméabilité de ces organes d'emménagement d'information soient suffisamment strictes pour protéger les renseignements qui nous concernent. C'est peut-être toutefois là un sujet qu'il serait mieux de traiter dans le contexte de la Loi sur la vie privée. Je crois que vous y avez également fait allusion, monsieur Spitzer, que vous avez dit qu'il nous faut parfois pouvoir avoir accès à certaines informations sur nous-mêmes. Il en va toutefois de même pour les dossiers d'employés tenus manuellement, par exemple, et l'on ne fait pas de distinction entre les données informatisées et les données consignées manuellement.

Peut-être devra-t-on revenir sur cette question un autre jour car il y en a beaucoup d'autres. En attendant, nous pourrions peut-être éliminer au moins une lacune en revenant à la question de l'accès non autorisé à un ordinateur. Dans tous les exemples que vous nous avez donnés, messieurs, on aurait pu au moins porter une accusation contre ces gens qui avaient à votre avis commis une infraction.

Je prie mes collègues de m'excuser d'être aussi long mais j'aimerais encore poser deux autres questions. Tout d'abord, l'obligation de signaler l'infraction. M. Spitzer a signalé que pour les infractions punissables, on est obligé de les rapporter.

[Texte]

indictable offence? Should any computer law have the requirement that an institution whose computer was violated would have to report it?

I gather that the greatest objection to that comes from two sources. One of them is universities, who like to be *in loco parentis* and do not like the idea of having the law necessarily apply to people on their grounds; secondly, from institutions, as you have pointed out, for whom there would be negative publicity.

If no serious damage was done to the data base, no serious loss of computer time, should there still be mandatory reporting?

Mr. Gentleman: I think there is another issue also which would cause people to object, which is the advent of distributed computing. As long as the computer was one big thing in one big building and you could afford to have people to monitor something like that then it would be practical. It would be practical and it would be an ethical question of whether you should or not. But in today's world, where it is just as likely that there are going to be 1,000 people carrying small computers as that there is going to be one large computer with some staff around it, it may very well be simply impractical to enforce any kind of auditing that would leave you in the place where you were able to report many of the incidents that would occur.

Mr. Spitzer: But that raises the same issue because if it is not an indictable offence then it is not an offence for which criminal charges will be pressed. And forgive me, I think you are sailing around the issue. In other words, I am in agreement with your earlier comment that you have to intimidate; you have to have the tools available so that you can press charges. And if you can press charges, it presumably means that it is an indictable offence, and under those conditions I certainly would subscribe to the idea that it should be required that it should be reported. I agree with you that . . .

• 1710

Mr. Gentleman: I was not saying that should not be required, I was saying that there are three sets of people who might drag their heels, not just two; and the third one is the people who would be inconvenienced by the fact that they have all these small distributed things and they would have to start monitoring them a lot more carefully than they do now.

Mr. Spitzer: I do not dispute that, but I am supporting what Mr. Beatty was suggesting, and that is that unless you have that requirement, a lot of this activity would go unattended.

Mr. Beatty: The other question may have resolved itself because I have forgotten it. I can perhaps come back to it later on.

Mr. Robinson (Etobicoke—Lakeshore): One of the things that I find confusing is the terminology that is being used and the fact that definitions are so important. I think it is danger-

[Traduction]

Qu'arrive-t-il s'il ne s'agit pas de les rapporter? Qu'arrive-t-il si ne s'agit pas d'une infraction punissable? Une loi sur les ordinateurs ne devrait-elle pas stipuler qu'un établissement qui a un ordinateur auquel quelqu'un a eu accès sans autorisation devrait le signaler?

Je crois que la plus grosse objection vient de deux sources. D'une part les universités qui aiment se situer *in loco parentis* et n'apprécient pas que la loi s'applique nécessairement sur leur terrain; deuxièmement, les établissements pour qui, comme vous le disiez, cela serait de la mauvaise publicité.

Si la base donnée n'était pas sérieusement endommagée, s'il n'y a pas de perte de temps d'ordinateur, ce rapport doit-il être rendu obligatoire?

M. Gentleman: Je crois qu'il y a également une autre question qui pousserait à faire objection à une telle disposition. Le fait que maintenant l'informatique est partagée. Tant que l'ordinateur était une grosse machine dans un grand bâtiment et que l'on pouvait avoir des gens pour surveiller, c'était possible. Cela aurait été possible et serait revenu à une question d'éthique. Toutefois, dans le monde d'aujourd'hui, il peut y avoir tout aussi bien 1,000 personnes avec de petits ordinateurs qu'un gros ordinateur utilisé par un personnel spécialisé et il est donc tout simplement impossible de procéder à quelque type de vérification qui vous permette de rapporter nombre des incidents qui se produisent.

M. Spitzer: Cela soulève la même question car s'il ne s'agit pas d'une infraction punissable, on ne peut porter d'accusations criminelles. Excusez-moi, je pense que vous tournez autour du pot. Autrement dit, je suis d'accord avec ce que vous disiez tout à l'heure, il faut exercer des pressions, vous avez besoin de pièces à conviction si vous voulez trouver un chef d'accusation. Si vous réussissez, cela veut dire qu'il y a délit et dans ces conditions je serai d'accord avec vous pour dire que l'on devrait exiger qu'une plainte soit déposée. Je suis d'accord avec vous pour dire que . . .

M. Gentlemen: Je ne disais pas qu'il ne fallait pas l'exiger, je voulais dire qu'il y avait trois sortes de gens qui pourraient se montrer peu disposés à coopérer et non pas simplement deux catégories; la troisième regrouperait précisément tous ceux qui seraient très gênés, du fait qu'il y aurait une telle dissémination qui exigerait une surveillance beaucoup plus sérieuse que ce n'est le cas pour le moment.

M. Spitzer: Je n'en disconviens pas, mais je soutiendrai en même temps que M. Beatty, qu'à moins d'avoir une exigence comme celle-là, on continuera à très peu surveiller toute cette activité.

M. Beatty: Mon autre question a peut-être reçu une réponse, en tout cas je l'ai oubliée. Peut-être y reviendrais-je tout à l'heure.

M. Robinson (Etobicoke—Lakeshore): Je suis très gêné par la confusion qui peut régner dans la terminologie, étant donné par ailleurs l'importance des définitions. Je pense qu'il est

[Text]

ous, say even for people like you, to be bandying about words like "indictable" and so on, without putting it in the proper context. For instance, if you are talking about an indictable offence, so-called, you are really talking about the way the person is going to be charged: whether they are going to be charged on indictment or they are going to be charged summarily. It depends on the severity of the offence and what is involved and so on, and it is up to the police to decide which way they want to charge, and it is up to the Crown attorney to decide whether he is going to proceed by way of indictment or summarily.

It becomes very confusing when we start talking about the jargon of one profession as against the jargon of another. But I have to admit to having a lack of knowledge and a lack of knowing the jargon of what this is really all about, when we start talking about computers and computer science and computer technology, and so on. There is so much for us to really learn, to really know what we are talking about, because we are not necessarily using the proper terminology, although we have some idea that we are trying to get across.

I have listened to both of you, and I have looked at the paper that you supplied, Mr. Spitzer, and it seems to me that really the basic problem is one of definition to start with; that without having proper definitions we cannot really cope with any of the other inherent problems that are there. Would you agree with that, that that is probably the...? You are nodding your head yes. If you could put it on the record by saying so, it will help.

Mr. Spitzer: I concur, yes.

Mr. Robinson (Etobicoke—Lakeshore): You concur with that.

Mr. Spitzer: I believe I stated so, in fact.

Mr. Robinson (Etobicoke—Lakeshore): You have also listed what might be a number of problems. What I am trying to get at at the moment is: What are the basic problems, or what is the major problem? I know there are many problems, but what do you consider as the major problem? Is it the security of the information in the computer? Is it the abuse to which a computer may be used? Is it the terminology that is not understood? Is it the fact that there is no law covering what we are really talking about?

Mr. Spitzer: If you wish me to give you one single answer, I will go for the last one. But basically, the entire Criminal Code, as currently tabled, does not have any opportunity for application when computers are used, either as the instrument or as the object of most criminal offences. The only exception that I am aware of is the law related to mischief.

Mr. Robinson (Etobicoke—Lakeshore): So what you are suggesting then is there would have to be a complete revision of the Criminal Code in many, many sections in order to accommodate "computer crime"—putting the term in quotes as you have done in your paper as a matter of fact—and along with that, I suppose, having special legislation.

[Translation]

dangereux, même pour des gens comme vous, de jouer avec des termes comme «délits punissables» etc., sans remettre les choses dans leur contexte. Par exemple, si l'on parle de «délits punissables», cela revient également à parler de la façon dont la personne concernée va être poursuivie: selon la procédure de l'acte d'accusation ou par simple déclaration sommaire de culpabilité. Tout dépend de la gravité du délit, et il appartiendra à la police de décider quel type de procédure elle suivra, et ensuite au procureur de la Couronne de savoir s'il va procéder par mise en accusation ou par simple déclaration sommaire de culpabilité.

Les choses deviennent extrêmement confuses lorsqu'on commence à opposer le jargon d'une profession à celui d'une autre. Mais j'admets mon manque de connaissance, notamment en ce qui concerne la terminologie consacrée, lorsque l'on commence à parler d'ordinateur, d'informatique et de technique informatique etc. Il y a tant à apprendre, et il arrive très souvent que nous n'utilisons pas les termes consacrés comme il le faut, même si nous avons une petite idée de ce que nous voulons dire.

Je vous ai écouté tous les deux, et j'ai regardé votre texte, monsieur Spitzer, et il me semble bien qu'un des problèmes de base soit celui des définitions; sans définition nous ne pourrions jamais résoudre les problèmes. Seriez-vous d'accord avec cela c'est très certainement... je vois que vous faites oui de la tête. Si vous pouviez le dire de façon explicite, pour que le compte rendu en porte la trace, j'en serais heureux.

M. Spitzer: Je suis d'accord, oui.

M. Robinson (Etobicoke—Lakeshore): Vous êtes d'accord avec cela.

M. Spitzer: Je pense l'avoir déjà dit.

M. Robinson (Etobicoke—Lakeshore): Vous avez également fait une liste d'un certain nombre de problèmes. Pour le moment, j'aimerais savoir ceci. Quels sont les problèmes les plus fondamentaux, où le problème le plus grave? Je sais qu'ils sont nombreux, mais que considérez-vous comme étant le problème central? Est-ce celui de la sécurité des renseignements enmagasinés dans l'ordinateur? Est-ce celui des abus auxquels peut donner lieu l'utilisation de l'ordinateur? Est-ce celui d'une terminologie qui reste incomprise? Est-ce le fait qu'il n'y ait pas de loi prévue à cet effet?

M. Spitzer: Pour vous donner une réponse simple, je dirais que c'est ce dernier problème qui compte le plus. Mais fondamentalement, c'est tout le Code criminel, comme il existe à l'heure actuelle, qui est totalement insuffisant lorsque l'on parle d'ordinateur comme instrument ou comme cible de délits criminels. À une exception près, je pense à la loi sur le méfait.

M. Robinson (Etobicoke—Lakeshore): Vous nous dites donc qu'il faudrait revoir complètement le Code criminel, du moins un nombre important de ses articles, pour pouvoir faire face à cette question du «crime informatique»—je mettrai ce terme entre guillemets, comme vous l'avez fait dans votre mémoire—et parallèlement à ce travail il faudrait donc adopter un ensemble de lois prévues à cet effet.

[Texte]

Mr. Spitzer: That is, I think, what I have tried to say in my brief. I have highlighted a number of areas where I am advised that there are specific problems, and I am just trying to put my finger very quickly on it. Somewhere I have, in fact, said that the problem is, indeed, the issue. We all know what is meant by theft of time; we all know that that is a wrong thing. We all know data trespass, or whatever term you want to use; that that is a wrong thing, but it is not defined in the legal context. And so on.

So yes, the mechanism by which the Criminal Code is rewritten is a separate issue, and I do not believe that the best vehicle for rewriting the Criminal Code is something which I am qualified to sit here and give any answers to.

• 1715

Mr. Robinson (Etobicoke—Lakeshore): But at the present time you are satisfied that the Criminal Code sections, as you understand them, would not be effective to stop computer crime.

Mr. Spitzer: That is the advice I have been given by several legal opinions with whom I have spoken.

Mr. Robinson (Etobicoke—Lakeshore): Maybe Mr. Gentleman would like to answer this, which is just a follow-up from that. You referred to the McLaughlin case and the fact that a computer was found not to be a telecommunications device. If it is not, then what is it? How do you classify it?

Mr. Gentleman: I think that was simply a mistake. I think a computer is a piece of telecommunications equipment. A computer is a telecommunications device.

Mr. Robinson (Etobicoke—Lakeshore): So the judge got bad information or bad advice, and made a bad judgment.

Mr. Gentleman: Yes.

The Chairman: May I just inquire when the judgment took place? I mean, some of the technology we know now was not even in existence.

Mr. Gentleman: That is partly related to it. The way most people thought of computers five years ago, ten years ago, fifteen years ago was very different from the way we think of them today.

The Chairman: They were autonomous entities and more or less able to be located, identified and controlled in a different fashion than they are today, because today on-line, multi-use and multiple-access is much more the trend. But when the honourable judges rendered their judgment, the technology was not really developed to the point we could foresee.

Mr. Gentleman: That is part of it. The other part of it is that the people who are at the leading edge of the technology may very well have a different view of it than does the general public, or what the judge was legally advised.

[Traduction]

M. Spitzer: Voilà ce que j'ai essayé de montrer dans mon mémoire, je pense. J'ai mis en évidence un certain nombre de domaines ou un certain nombre de problèmes bien précis qui se posent et j'essaie rapidement d'attirer votre attention là-dessus. J'ai expliqué quelque part que le problème est celui de la définition même de la question. Nous savons tous ce que veut dire voler du temps; nous savons que c'est mal. Nous savons également ce que peut-être le viol du secret, quel que soit le terme que vous utilisiez; nous savons également que c'est mal, mais tout cela n'est pas défini de façon juridique. Etc. etc.

Donc, oui, la refonte du Code criminel est une question à part, et je ne pense pas que je sois ni qualifié ni présent ici pour donner une réponse sur la meilleure façon de s'y prendre.

M. Robinson (Etobicoke—Lakeshore): Mais vous êtes convaincu à l'heure actuelle que les dispositions du Code criminel ne seraient pas efficaces pour supprimer le crime informatique.

M. Spitzer: C'est ce que m'ont donné à entendre plusieurs juristes avec lesquels j'ai parlé.

M. Robinson (Etobicoke—Lakeshore): M. Gentleman voudra peut-être répondre à ma prochaine question qui découle de la précédente. Vous avez parlé de l'affaire McLaughlin et de la décision selon laquelle un ordinateur n'est pas un dispositif de télécommunication. Si l'ordinateur n'est pas un dispositif de télécommunication, qu'est-ce que c'est? Comment le classez-vous?

M. Gentleman: Je pense que ce fut une erreur. L'ordinateur est une pièce d'équipement de télécommunication. L'ordinateur est un dispositif de télécommunication.

M. Robinson (Etobicoke—Lakeshore): Alors le juge a été mal renseigné, mal conseillé et a rendu une mauvaise décision.

M. Gentleman: Oui.

Le président: Quand cette décision a-t-elle été rendue? Certaines technologies que nous connaissons aujourd'hui n'existaient même pas à ce moment-là.

M. Gentleman: Cela explique en partie les problèmes. La façon dont on envisageait généralement l'ordinateur il y a 5 ans, 10 ans, ou 15 ans est très différente d'aujourd'hui.

Le président: Il s'agissait alors d'installations autonomes, et les moyens de les répérer, de les identifier et de les contrôler étaient plus ou moins différents de ceux d'aujourd'hui, compte tenu des systèmes directs, des systèmes à utilisation et à accès multiples dont nous disposons aujourd'hui. Mais lorsque les honorables juges ont rendu leur décision, la technologie n'était pas aussi avancée quelle l'est aujourd'hui.

M. Gentleman: C'est une partie de l'explication. L'autre partie est que les personnes qui sont à la fine pointe de la technologie peuvent très bien avoir une conception de l'ordinateur qui diffère de celle du grand public ou de celle que les juges se sont faites après consultation.

[Text]

The example I quoted is that of one of the major American computer manufacturers which has viewed itself not as being in the computer business but being in the communications business, and their whole computer systems are designed from the point of view of that this is communicating people-to-people, though maybe with a delay in time, and in fact dates from 1965 and from a computer manufacturer who is not normally thought of as being related to telecommunications at all; most of their systems are not interactive systems. But in that company the perception of what they were doing existed in the minds of the people who were designing and building the products, and the products were built to that idea.

Mr. Robinson (Etobicoke—Lakeshore): Have either of you gentlemen considered the problem of somebody programming their computer in such a way that it contains false and inaccurate information? Take a formula, for example. Your competitor might want to know this particular formula, but you put it on your computer falsely. They take it, use it and as a result have a poor product, or somebody dies, depending on what kind what kind of information you put on the computer, and harm, damage or injury results.

Mr. Gentleman: I had that very much in mind when I referred to the problem of the computer as a communications device spreading false information. I think it is very likely to see that happen. I am not sure that I can remember any specific instance where it has, but I would not even be surprised that if I tried hard enough I could find such an instance.

Mr. Robinson (Etobicoke—Lakeshore): I suppose you would analogize that to the trespasser who comes onto your property and falls down a well. You owe a duty not to leave the cover off the well so that a trespasser could fall down the well and drown. You owe some kind of a duty. What I am trying to determine is what duty you feel is owed by the owner or the programmer of the computer to people who might break into the computer bank or take the information out of it. They are committing a crime. When we have legislation covering it, we are going to say that they have committed a crime. But what about you, as the owner or programmer?

Mr. Spitzer: I would like to suggest that the concept of caveat emptor applies. When you take the analogy of the well on your property, if you have a sign up which says 'thou shalt not enter; enter at your own peril'—which is what you are effectively doing the moment you put a security system on a computer, saying I have passwords and so on—after that, I believe I have no responsibility, in the legal concept, if somebody falls down the well. That is their misfortune. I would suggest that if a company is foolish enough to rip off from my computer the wrong formula for my new toothpaste and it turns everybody's teeth black, I think they have got a poor lookout coming for them. I would venture the suggestion, since you asked my opinion, that I have no responsibilities toward them.

[Translation]

L'exemple que je vous ai donné est celui de grands fabricants américains d'ordinateurs qui se sont toujours considérés comme évoluant non pas dans le domaine de l'informatique mais dans celui des communications, et tous leurs systèmes informatiques sont conçus en fonction du principe de communication directe entre personnes, bien qu'il faille remonter un peu dans le temps, en fait jusqu'en 1965; mais du côté des fabricants d'ordinateurs, qui ne sont pas considérés normalement comme faisant partie du secteur des télécommunications, la plupart des systèmes ne sont pas interactifs. Mais dans cette compagnie, les concepteurs et les fabricants des produits envisageaient l'informatique comme un secteur de communication, et bâtissaient leurs produits en fonction de ce principe.

M. Robinson (Etobicoke—Lakeshore): Avez-vous déjà pensé à la possibilité que quelqu'un puisse programmer leur ordinateur en y insérant de l'information erronée et inexacte? Prenez une formule par exemple. Votre concurrent sera peut-être intéressé à l'avoir, mais vous l'intégrez à votre ordinateur avec des erreurs. Votre concurrent s'en empare et l'utilise et comme résultat, il obtient un mauvais produit, ou quelqu'un meurt, selon le genre d'information que vous mettez dans l'ordinateur.

M. Gentleman: J'avais beaucoup de choses en tête lorsque j'ai parlé du problème de l'ordinateur comme dispositif de communication susceptible de disséminer de la fausse information. Je pense qu'il est très probable que cela se produise. Je ne me souviens pas exactement d'un exemple précis où cela se serait produit, mais je ne serais pas étonné d'en trouver si je faisais l'effort voulu.

M. Robinson (Etobicoke—Lakeshore): Vous pourriez probablement établir un parallèle avec quelqu'un qui s'introduit sur votre propriété sans autorisation et qui tombe dans un puits. C'est votre devoir de ne pas laisser le puits à découvert pour ne pas qu'une personne y tombe. C'est votre responsabilité. Ce que j'essaie de déterminer, c'est quelle est selon vous la responsabilité du propriétaire ou du programmeur de l'ordinateur envers les personnes susceptibles de pénétrer la banque informatique ou d'y prendre de l'information. Ces personnes commettent un crime. Lorsque la loi sera en place, nous pourrions dire que ces gens-là ont commis un crime. Mais qu'en pensez-vous en tant que propriétaire ou programmeur?

M. Spitzer: Je pense que le principe de l'avertissement s'applique ici. Pour reprendre votre analogie du puits sur votre propriété, si vous avez un avertissement qui dit Interdit d'entrer, entrez à vos propres risques et périls... ce que vous faites effectivement dès que vous intégrez un système de sécurité à l'ordinateur, vous dites que vous avez un mot de passe et ainsi de suite... Après cela, je pense que vous ne pouvez plus être responsable, dans le sens légal du terme, si quelqu'un tombe dans le puits. Ce n'est pas votre problème. Si une compagnie est suffisamment stupide pour extirper de mon ordinateur la fausse formule pour ma nouvelle pâte dentifrice et que les dents de leurs clients deviennent toutes noires, sa réputation doit en prendre un coup. Puisque vous me demandez mon avis, j'estime n'avoir aucune responsabilité.

[Texte]

• 1720

Mr. Robinson (Etobicoke—Lakeshore): But suppose you leave the cover off the well, knowing that people will—in spite of the fact you have signs around saying beware of the well... be prowling around; or if they prowl around at night and they do not see the signs that are up, do you not owe some duty? Is there not some duty of care on your part, if you are dealing with a computer, to protect what you have and to make sure that you do not, you know, put false information on it, that somebody might get and use?

Mr. Spitzer: I think we dealt with this issue in a separate context, where I made reference to it in the concern I had that one has to ensure that only people who should have access to a machine, do have access to a machine. Once you have provided them with the correct information your burden of responsibility, I would suggest, is to protect it. Protect the machine from other people getting on. And the Criminal Code would, I think, be wrongly drafted if it laid blame that my competitor produces black toothpaste, as it were.

Mr. Robinson (Etobicoke—Lakeshore): I was hoping that either one of you would suggest that this would be one of the ways of safeguarding your information; by putting false information. That is one of your safeguards; it is one of your security measures. So only you know what part of it is false; only you can change it.

Mr. Spitzer: Forgive me, sir, I think the complexities of running a large-scale data processing facility or any computing facility are sufficiently substantial that one does not, unless one has a reason, plant trouble. And I will go back to the Dalton School situation, if I may again, in which I understand the children from that school successfully entered and used the machine operated by Canada Cement Lafarge Ltd. in Montreal. That was a plant. It was known that those kids were tampering; they were given access and the damage they caused was carefully controlled damage. That was a plant, if you will; that was an enticement. Certainly I have done that, but I have done it as a mechanism of investigation and I believe that even as a method of investigation, in the criminal courts, the concept of putting temptation in people's way has sometimes been raised as a mechanism of defence.

Mr. Robinson (Etobicoke—Lakeshore): Yes, you are quite right on that.

Mr. Gentleman: I can provide you with a slightly different answer, and that is that providing wrong or misleading information as a defence mechanism is in fact possible. The statistical world and agencies such as Statistics Canada and the U.S. Census Bureau deliberately have to do that, for legal reasons. It is very hard to do and I think it is, in fact, unrealistic to expect that normal data processing activities would be able to or be prepared to pay the overhead in doing that in such a way that some questions would get answered wrongly, and the questions that were important to get answered rightly would in fact get answered rightly.

Mr. Beatty: It is commonly done for both copyright and patent purposes. Copyright with directories. The student directory at the University of Waterloo; the students' council

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Si vous ne bouchez pas le puits, sachant qu'il va y avoir des rôdeurs, malgré que vous ayez mis des panneaux d'avertissement, ou si ces rôdeurs viennent la nuit et ne peuvent par conséquent voir ces panneaux, n'êtes-vous pas un peu responsable? Si vous avez un ordinateur, n'avez-vous pas la responsabilité de protéger ce qu'il contient et de ne pas y faire entrer de faux renseignements qui pourraient être utilisés par quelqu'un?

M. Spitzer: Je crois qu'il s'agit d'un contexte différent. J'ai dit qu'il fallait s'assurer que seules les personnes autorisées aient accès à la machine. Une fois les personnes autorisées renseignées correctement, la seule responsabilité restante, à mon avis, est de protéger la machine contre les personnes non autorisées. Que le Code criminel m'incrimine parce que mes concurrents fabriquent de la pâte dentifrice noire, serait injuste.

M. Robinson (Etobicoke—Lakeshore): J'espérais que l'un d'entre vous suggérerait qu'informatiser de faux renseignements serait un des moyens de protéger ces renseignements informatisés; que c'est une de vos défenses, une de vos mesures de sécurité. Vous seriez les seuls à savoir ce qui est faux et vous seriez les seuls à pouvoir le changer.

M. Spitzer: Je m'excuse, monsieur, mais exploiter un système informatisé est déjà suffisamment compliqué pour ne pas ajouter des complications supplémentaires sans de bonnes raisons. Permettez-moi de revenir à ce qui s'est passé à l'école Dalton où si je comprends bien les élèves ont réussi à percer le code de l'ordinateur des Ciments Lafarge de Montréal et à s'en servir. On savait ce que faisaient ces enfants et ils n'ont pu causer que des dommages soigneusement contrôlés. C'était en quelque sorte un exercice, si vous voulez, on les y avait incités. C'est ce que j'ai fait moi-même, mais dans un but d'enquête et je crois que même comme méthode d'enquête, la notion de provocation a parfois été revendiquée comme moyen de défense devant les tribunaux.

M. Robinson (Etobicoke—Lakeshore): Oui, vous avez tout à fait raison.

M. Gentleman: Je peux vous donner une réponse un peu différente. Fournir des renseignements faux ou erronés comme moyen de défense est en fait possible. Le monde des statistiques et des agences comme Statistique Canada et le Bureau de recensement des États-Unis le font délibérément, pour des raisons juridiques. C'est très difficile à réaliser, et je pense en fait qu'il n'est pas réaliste de croire que les compagnies soient prêtes à faire des dépenses supplémentaires dans leur programme informatique pour faire en sorte que les réponses à certaines questions soient fausses et que les réponses aux questions importantes demeurent justes.

M. Beatty: Cela se fait couramment pour les droits d'auteur et les brevets. Cela se fait dans les annuaires de droits d'auteur. L'annuaire des étudiants de l'Université de Waterloo;

[Text]

likely includes in that phoney names and addresses. They know that if somebody sends a letter of solicitation to the phoney person included there, that they have broken copyright.

From the point of view of patent or of protection of a . . . I will give you one example. It is of a computer chip designed in the U.S., where the designer deliberately put a little blip in the side which had no instructive purpose. Subsequently, in reading a Russian scientific publication taking credit for a new computer chip the Soviets had designed, he discovered that his particular signature had been included in the design of the computer chip. It had shown up and it was his way of establishing that in fact his rights to the property had been damaged. So it is not uncommon to include redundant or false information as a means of identifying . . .

Mr. Gentleman: I do not say you cannot do it, but as a general mechanism it is very hard to do.

Mr. Spitzer: And redundant is different from false.

• 1725

Mr. Beatty: But it is common with computer programs, is it not, that you can put a signature into a computer program in a number of different ways. One is by the order of arrangement that you would have it in, which might be unique. Another would be by adding information which is not integral to the function of the program itself; and you know if you see a copy with that in, someone would not spontaneously have come up with that.

Mr. Spitzer: That is precisely it; it is redundant.

Mr. Robinson (Etobicoke—Lakeshore): What you are really saying is that there could be a built-in entrapment mechanism in your program, and this might be part of your security. Would that be fair to say?

Mr. Spitzer: Yes.

Mr. Robinson (Etobicoke—Lakeshore): You have suggested—I think both of you have—that there are some people who should probably not be allowed to use computers, and there are certain people who obviously should be allowed to use computers. Are you suggesting in some way that there should be a licensing process to use computers or to have computers; somewhat like having a licence to drive a car, or having ownership to own a car?

Mr. Gentleman: I do not think I would agree at all that there are people who should be able to use computers and people who should not be able to use computers. I do not see any reason, for instance, to prevent someone from using a microwave oven because it happens to have a computer in it.

What I think we have said is that, for any given computer, it is probably desirable to restrict who has access to it. Even something like this might contain information—and again, the example I actually saw last week was that the executives of a major American company were all wandering around with these things with the financial figures for their companies in them. You definitely do not want to leave those so that any

[Translation]

le conseil des étudiants inclut vraisemblablement de faux noms et de fausses adresses. Ils savent que si quelqu'un envoie une lettre de sollicitation à la fausse adresse qu'il y a violation de droits d'auteur.

Pour ce qui est de la protection des brevets . . . Je vais vous donner un exemple. Il s'agit d'une puce conçue aux États-Unis à laquelle le concepteur a délibérément ajouté un élément inutile. Subséquemment, en lisant un article dans une revue scientifique russe annonçant l'invention d'une nouvelle puce, il a découvert qu'elle contenait cet élément inutile. Il a pu ainsi démontrer qu'on avait copié sa propre invention. Il n'est donc pas rare d'inclure de faux renseignements ou des renseignements redondants permettant d'identifier . . .

M. Gentleman: Je ne dis pas que vous ne pouvez pas le faire, mais que d'une manière générale c'est très difficile à réaliser.

M. Spitzer: Et il y a une différence entre redondant et faux.

M. Beatty: Mais les programmes d'ordinateurs ne comportent-ils pas généralement une signature? Une façon de faire c'est d'avoir un arrangement qui soit unique. Une autre façon est d'ajouter des renseignements qui ne font pas partie intégrante du programme comme tel; et si vous voyez un imprimé où ces renseignements apparaissent, alors vous savez que quelqu'un ne les pas obtenus par hasard.

M. Spitzer: C'est précisément cela, c'est redondant.

M. Robinson (Etobicoke—Lakeshore): Ce que vous dites en réalité c'est que votre programme pourrait comprendre un mécanisme piège et cela ferait partie de votre système de sécurité. N'est-ce pas?

M. Spitzer: En effet.

M. Robinson (Etobicoke—Lakeshore): Tous les deux, je pense, vous avez suggéré qu'il y a certaines personnes à qui l'on devra probablement interdire d'utiliser des ordinateurs et il y en a d'autres à qui on devra évidemment permettre la chose. Proposez-vous la délivrance de permis d'utilisation ou de possession d'ordinateurs, à l'instar du permis de conduire ou de l'enregistrement de voitures?

M. Gentleman: Je ne pense pas que je sois du tout d'accord sur cette proposition que certaines personnes devraient avoir le droit d'utiliser les ordinateurs et d'autres non. Par exemple, je ne vois aucune raison pour interdire à quiconque d'utiliser un four à micro-ondes simplement parce qu'il est doté d'un ordinateur.

Ce que nous avons dit, je pense, c'est que pour tout ordinateur, il est probablement souhaitable de restreindre le nombre de personnes qui y ont accès, à cause des renseignements qui y sont contenues . . . Et encore une fois, je vous donne comme exemple, quelque chose que j'ai réellement vu la semaine dernière, alors que des cadres d'une grande compagnie américaine se balladaient avec ces appareils contenant des

[Texte]

person can flip the switch and power it on and read them. Even something as simple as this, there should be some kind of access control in. But I do not think I can imagine a person who is so evil that they should not be able to use any computer at all, ever, anywhere.

Mr. Robinson (Etobicoke—Lakeshore): Well, there is the potential damage that they can cause. We do not allow just everybody to drive a car. You are expected to have a licence because you are expected to know how to use it. It is like having a gun: you need to know how to use it and how to use it properly and be a responsible person. Do you not think the same kind of rules should apply to computers?

Mr. Gentleman: No. I do not know anything useful that I could put in the licensing requirement.

Mr. Robinson (Etobicoke—Lakeshore): I see.

My last question, then, will be on the enforceability of the law that might be applied. You did mention that it certainly should not be obsolete, and with the fast-moving technology these days we would probably have to keep a monitor on it to keep it up to date. But the enforceability is another matter; and when you couple that with the immense problem of detection, you have the whole problem of enforceability. I just wonder what we are really talking about as far as enforceability is concerned.

Somebody mentioned the seat-belt laws. Well, it is virtually impossible to enforce the seat-belt laws unless the police were at every corner, stopping everybody all the time. Maybe through an educational program you have some impact. But how do you enforce it, really and truly? And how would we be able to enforce this one, when you cannot even detect when the crime is being committed?

Mr. Gentleman: I think that is why we both referred to the observation that intimidation seems to be the most successful way of actually encouraging people not to behave in an anti-social manner. It is very easy to get around most of the things that we are capable of doing—of detecting that a crime has occurred—a computer crime, quote—of identifying that something really is the same thing as was stolen; of identifying who is the perpetrator. However, we all have histories of having managed by sheer blind accident, in many cases . . . of having stumbled across enough cases where in fact the perpetrator is quite ready to admit he did it. So, having some kind of legal backing to say that, in the cases where we do accidentally stumble over that, we have the ability to extract some sort of retribution, the effect is going to deter other people. We cannot hope to defeat the people who are really determined because as far as we can see, the technology is such that somebody who is really determined is not going to be

[Traduction]

données financières de leur compagnie. Il va sans dire que vous ne voulez pas les laisser traîner à la portée de n'importe qui, car il suffit de mettre le commutateur et de lire les renseignements. Même pour quelque chose d'aussi simple que cela, il faudrait en quelque sorte contrôler l'accès. Mais je ne peux pas m'imaginer qu'une personne soit tellement dangereuse qu'elle devrait se voir interdire l'accès aux ordinateurs quels qu'ils soient, où que ce soit.

M. Robinson (Etobicoke—Lakeshore): Bien, il y a les dommages qui peuvent être causés. Nous ne permettons pas à tout le monde de conduire une voiture. On s'attend à ce que vous ayez un permis de conducteur car on s'attend à ce que vous sachiez conduire. C'est la même chose pour une arme: il est nécessaire que vous sachiez comment l'utiliser, comment bien l'utiliser et que vous soyez une personne responsable. Ne croyez-vous pas que le même genre de règles puisse s'appliquer aux ordinateurs?

M. Gentleman: Non. Je ne vois rien d'utile que je pourrais inclure comme exigence pour l'obtention d'un permis.

M. Robinson (Etobicoke—Lakeshore): Je vois.

Alors, ma dernière question portera sur la possibilité d'appliquer une loi, le cas échéant. Vous avez dit qu'une loi en ce sens ne devrait pas être dépassée et que, compte tenu de la vitesse du progrès technologique de nos jours, nous devrions probablement surveiller les choses de près pour que cette loi soit toujours d'actualité. Mais la possibilité de l'appliquer est une autre chose et lors que vous y ajoutez l'immense problème de détection, alors vous avez l'ensemble du problème pour ce qui est de la possibilité d'appliquer une loi. En fait, je me demande réellement de quoi nous parlons lorsque nous parlons de la possibilité d'appliquer une loi.

Quelqu'un a fait allusion aux lois visant les ceintures de sécurité. Bien, il est virtuellement impossible d'appliquer les lois sur les ceintures de sécurité à moins d'avoir, à chaque coin de rue, des agents de police arrêtant tout le monde tout le temps. On peut-être avoir un certain résultat par le truchement d'un programme d'éducation. Mais comment peut-on réellement l'appliquer? Et comment pourrions-nous appliquer celle-ci alors qu'on ne peut même pas déceler quand le crime est commis?

M. Gentleman: Je pense que c'est pourquoi nous avons tous deux fait allusion au fait que l'intimidation semble être la façon la plus prometteuse d'encourager les gens à ne pas se comporter de façon antisociale. Il est très facile d'éviter la plupart des choses que nous sommes en mesure de faire . . . Déceler qu'un crime a été commis . . . un crime par ordinateur, déterminer que quelque chose a réellement été volé; ou identifier le responsable. Toutefois, nous pouvons tous vous raconter nombre de cas où nous avons réussi par pur hasard, dans bien des cas . . . Nous sommes tombés sur suffisamment de cas où en fait le responsable était vraiment prêt à reconnaître son forfait. Compte tenu de ce que je sais sur le plan juridique, dans les cas où nous sommes confrontés à ce genre de choses, nous sommes en mesure d'obtenir une forme de sanction, ce qui aura un effet dissuasif. Toutefois, nous ne pouvons espérer faire échec à ceux qui sont vraiment déterminés parce que pour autant que nous le sachions, la technologie

[Text]

detectable; you are not going to know that they took something, and even if you did know they took it, you are not going to be able to prove that what they took is the same as the original.

• 1730

Mr. Spitzer: I concur and I would like to carry on again with analogies. We have used them a lot. The salutary effect on everybody's driving habits of seeing a police car sitting with a dummy in it over the Labour Day weekend has been proven by many police forces throughout the States. In the same way, collecting one person every now and again and providing public example of the enforcement of the law, like this, is likely to have a salutary effect, I would think, on a wider basis than one could hope for by directly enforcing it.

The Chairman: Thank you gentlemen.

Before we conclude, may I ask how much the small computer you have is costing?

Mr. Gentleman: All right. The simple answer to that is that, including tax, at your friendly neighbourhood Radio Shack store it is \$1,502 and, if instead you were buying it at your friendly neighbourhood radio store on the other side of the border, in the United States, it would be about half that.

Mr. Beatty: Do you get a commission for that commercial?

Mr. Gentleman: I have no intention of owning this.

Mr. Robinson (Etobicoke—Lakeshore): All Canadians should go across the border and buy their computer.

Mr. Gentleman: You should have an indigenous industry here.

The Chairman: Anyway, thank you for helping us in our reflection and for coming this afternoon and appearing before the committee. I would like to say that the next subcommittee will resume next Tuesday, May 17, at 9.30 a.m. at Room 208 with Mr. Dave Conway and Mr. Tony Guliani from Mitel Corporation.

I thank you. The meeting is adjourned.

[Translation]

en usage permet à quelqu'un de vraiment déterminé de prendre certaines dispositions impossibles à déceler. Cela signifie donc qu'on ignorera qu'il a volé quelque chose, et même si on le sait, on sera incapable de prouver que ce qui a été volé correspond à l'original.

M. Spitzer: Je suis d'accord et j'aimerais encore une fois recourir à des analogies comme nous l'avons souvent fait. Pensons par exemple aux effets salutaires sur la conduite automobile de tous les citoyens de la présence d'un mannequin assis dans une voiture de police pendant la fin de semaine de la Fête du Travail; cela a même été documenté par bon nombre de corps policiers, partout aux États-Unis. De la même manière, l'arrestation d'une personne de temps à autre sert d'exemple de mise en vigueur de la loi auprès du public, et cela aura probablement aussi des effets plus bénéfiques que l'application directe de sanctions.

Le président: Merci, messieurs.

Avant de conclure, puis-je vous demander combien coûte le petit ordinateur que vous avez avec vous?

M. Gentleman: C'est bien. Vous pouvez vous procurer cet ordinateur chez votre sympathique vendeur du magasin *Radio Shack* pour \$1,502 taxe comprise et si vous choisissez plutôt de l'acheter de l'autre côté de la frontière, aux États-Unis, il vous coûtera à peu près la moitié de cela.

M. Beatty: Recevez-vous une commission pour cette publicité?

M. Gentleman: Je n'ai nullement l'intention d'acheter celui-ci.

M. Robinson (Etobicoke—Lakeshore): Tous les Canadiens devraient traverser la frontière pour acheter leur ordinateur.

M. Gentleman: Il faudrait avoir notre propre industrie de l'informatique ici.

Le président: Quoiqu'il en soit, je vous remercie d'avoir fait avancer notre réflexion sur cette question et d'être venu témoigner devant nous cet après-midi. En terminant, je précise que la prochaine réunion du Sous-comité aura lieu le mardi 17 mai, à 9h30, à la salle 208 alors que nous accueillerons M. Dave Conway et M. Tony Guliani de la société Mitel.

Je vous remercie. La séance est levée.





*If undelivered, return COVER ONLY to
Canadian Government Publishing Centre
Supply and Services Canada
Ottawa, Canada, K1A 0S9*

*En cas de non-livraison
retourner cette COUVERTURE SEULEMENT à
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada
Ottawa, Canada, K1A 0S9*

WITNESSES—TÉMOINS

Mr. Morvin Gentleman, National Research Council;
Mr. Frank Spitzer, Consultant, Toronto.

M. Morvin Gentleman, Conseil national de la recherche;
M. Frank Spitzer, consultant, Toronto.

22

HOUSE OF COMMONS

Issue No. 8

Tuesday, May 17, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 8

Le mardi 17 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

*Procès-verbaux et témoignages
du Sous-comité sur*

Computer Crime

Les infractions relatives aux ordinateurs

of the Standing Committee on Justice and Legal Affairs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

CONCERNANT:

Matters pertaining to the Order of Reference

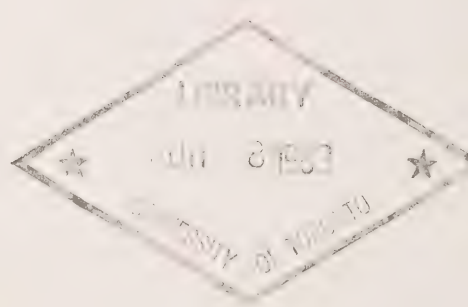
Questions relatives à l'ordre de renvoi

WITNESSES:

TÉMOINS:

(See back cover)

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

TUESDAY, MAY 17, 1983
(10)

[Text]

The Sub-committee on computer crime met this day at 9:58 o'clock a.m., the Acting-Chairman, Mr. Perrin Beatty, presiding.

Member of the Sub-committee present: Mrs. Céline Hervieux-Payette.

Designated Alternate Member Present: Mr. Beatty.

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: Mr. Dave M. Conway, Manager, Resources Protection, Mitel Corporation, Kanata, Ontario and Professor Tony J. Juliani, Department of Criminology, Ottawa University.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements.

The Chairman took the Chair.

The witnesses answered questions.

At 10:59 o'clock a.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MARDI 17 MAI 1983
(10)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 10h 58, sous la présidence de M. Perrin Beatty, président suppléant.

Membre du Sous-comité présent: M^{me} Céline Hervieux-Payette.

Membre substitut désigné présent: M. Beatty.

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: M. Dave M. Conway, gérant, protection des ressources, Mitel Corporation, Kanata, Ontario et Professeur Tony J. Juliani, Département de criminologie, Université d'Ottawa.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations.

Le président occupe le fauteuil.

Les témoins répondent aux questions.

A 10h 59, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Tuesday, May 17, 1983

• 0958

The Acting Chairman (Mr. Beatty): Ladies and gentlemen, perhaps I could call the meeting to order. The chairman is en route. She unfortunately had a flat tire and was delayed on her way here, but she is still coming. Mr. Robinson, I understand, is somewhere between his office and here. I am not sure of the route he is following. Perhaps we could start and give our witnesses the opportunity to make some initial comments and then when other members of the committee get here, we will be able to deal with the questions.

The witnesses today are Mr. David Conway of Mitel Corporation, Ottawa, and Professor Tony Juliani of the University of Ottawa.

Gentlemen, you have prepared a brief. Did you want to present it orally as well?

Mr. Tony Juliani (Department of Criminology, University of Ottawa): It would be best. Then we could entertain questions, if you so wish.

The Acting Chairman (Mr. Beatty): By all means. Please go ahead.

Mr. Juliani: What we have done is prepare a macro-perspective on the problem that was presented to us, and we have entitled it . . . *White Collar Crime*—mistakenly so, but I believe the comments apply to this particular committee. So we will give you the macro-perspective initially, and then David will entertain specific issues relevant to industrial security as in place at Mitel.

Members of the committee, white collar crime is usually associated with crimes committed by persons of responsibility and high status in the course of their occupations. Crimes involving employee theft, price fixing, infringement of patents, unfair labour practices, etc., serve to strike a mortal blow to public morality, because of the relative impunity with which such acts are committed and the relative leniency expressed by the judicial system. The illicit acts of apparently law-abiding individuals have a devastating effect on societal conception of morality, as the activity serves to blur the distinction between men and businessmen. This eroding process was described by President Johnson's Commission on Law Enforcement and the Administration of Justice in 1967 as follows:

• 1000

Derelictions by Corporations and their managers who usually occupy leadership positions in the communities establish an example which tends to erode the moral base of law and provide an opportunity for other kinds of offenders to rationalize their conduct.

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mardi 17 mai 1983

Le président suppléant (M. Beatty): Mesdames et messieurs, je vais ouvrir la séance. Le président est en route. Malheureusement, elle a eu une crevaïson, ce qui explique son retard; mais elle assistera à la réunion. D'après ce qu'on m'a dit, M. Robinson a quitté son bureau pour se diriger vers cette pièce. Je ne sais pas au juste s'il s'en vient directement. Nous pourrions commencer et donner aux témoins l'occasion de faire quelques déclarations préliminaires; lorsque d'autres membres du Comité seront là, nous pourrions passer à la période des questions.

Les témoins sont M. David Conway, de la *Mitel Corporation*, d'Ottawa, et M. Tony Juliani, professeur à l'Université d'Ottawa.

Messieurs, vous avez présenté un mémoire. Avez-vous l'intention de le lire également?

M. Tony Juliani (département de criminologie, Université d'Ottawa): Il vaudrait mieux le lire d'abord. Puis nous pourrions répondre à vos questions, si vous le voulez.

Le président suppléant (M. Beatty): Bien sûr, allez-y, je vous en prie.

M. Juliani: Nous avons étudié la question qui nous a été soumise dans son ensemble et nous avons intitulé nos résultats: «Délinquants commis par les cols blancs», à tort, mais il me semble que les observations intéresseront votre comité. Nous vous brosserons donc un tableau d'ensemble, pour commencer; puis David parlera de questions précises concernant la sécurité industrielle, notamment celles que la *Mitel* a relevées.

Membres du Comité, on entend habituellement par crimes des cols blancs ceux qui sont perpétrés par des personnes de haut rang ou qui ont de grandes responsabilités en raison du poste qu'elles occupent. Les crimes où il est question de vol par l'employé, de fixation des prix, de contrefaçon en matière de brevets, de pratiques déloyales envers la main-d'oeuvre, par exemple, finissent par asséner un coup mortel à la moralité publique, car ils sont perpétrés assez impunément, et le système judiciaire se montre assez indulgent. Les actes illicites d'individus qui, selon toute apparence, respectent la loi, ont un effet dévastateur sur la conception sociale de la moralité, étant donné que l'activité semble rapprocher les deux notions d'homme d'affaires et d'escroc. Ce phénomène a été décrit ainsi, en 1967 par la Commission du président Johnson sur l'application de la loi et l'administration de la justice:

Les manquements à leur devoir par les entreprises et leurs dirigeants, qui, habituellement, occupent des postes de direction dans les communautés, donnent un exemple qui a tendance à miner la base morale de la loi et fournissent à d'autres genres de criminels l'occasion de rationaliser leur comportement.

[Texte]

The investigation of individuals who committed crimes against corporations reveal them to be moral men who had what was considered an unshareable financial problem, who saw presented to them a means of solving that problem, and who are able to reconcile their concept of themselves as moral men with the concept of immorality generated by the act. The individual's willingness to victimize an organization is viewed as a function of the size of the organization, with people being more willing to steal from big business as opposed to small business.

In a study by the Pitney Bowes Corporation, the majority of managers of corporations were found to be willing to compromise personal ethics, to achieve corporate goals. In addition, in a further study by Madden, it is suggested that managers believe their peers would choose to mask defective and possibly dangerous products, and that younger managers automatically follow the practices of the more experienced managers, possibly due to loyalty. This seems to indicate that the morally abnormal behaviour is becoming the more acceptable standard, especially when considering that practices, generally referred to as fraud by the police, are defined by entrepreneurs as simply good business practices.

As examples of this type of behaviour, one has the case in the U.S. of the aircraft company which produced thousands of airplanes with defective fuel tanks, being responsible for numerous crash deaths, revealed the problem to be due to the reluctance of the controlling agency to intervene. And further, the case of the mining company indicated the problem to be the social impact of conforming, when the question was reduced to two alternatives—the possible danger to 150,000 consumers of polluted water and the actual distress to 32,000 employees possibly facing lay-off.

The leniency with which white collar criminals are dealt with by the courts, as well as the manner in which white collar criminals are prosecuted, has led to the claim that what the criminal justice system needs is a massive infusion of investigative and prosecutive resources to produce an increase in the volume of white collar offenders prosecuted. In addition, there seems to be a need for a revision of existing statutes in order to provide the possibility of increased sanctions. Increased penalties should have a positive effect in reducing recidivism because of the deterrent value of combatting white collar crime. Where deterrence has failed in reducing traditional criminality, deterrence has a definite role in reducing white collar crime in view of the type of offender engaging in this type of activity.

In dealing with the white collar offender, one is confronted with an individual who has been habilitated in terms of societal norms, for his successful climb to a position of authority and trust is a measure of that commitment. Therefore, if a potential offender is confronted with the real possibility of apprehension, conviction and subsequent loss of his career achievements, he will be more inclined to be deterred from engaging in unlawful behaviour. Being the intelligent and careful thinker that he is, the cost of his apprehension is

[Traduction]

Les enquêtes menées sur les personnes ayant commis des infractions contre des entreprises ont conclu qu'il s'agissait de personnes, ayant un sens moral, aux prises avec un problème financier qu'elles ne pouvaient pas partager, qui ont vu apparaître une solution possible à leur problème et qui s'estimaient encore pourvues de sens moral, malgré l'acte immoral commis. La volonté de l'individu de s'en prendre à une organisation est souvent fonction de l'importance de cette organisation; les gens démontrent moins de réticence à voler une grande entreprise qu'une petite.

Une étude faite par la *Pitney Bowes Corporation* a conclu que la majorité des dirigeants de sociétés semblaient enclins à transiger sur des questions d'éthique professionnelle pour atteindre les objectifs fixés par cette société. De plus, selon une autre étude entreprise par Madden, les dirigeants estiment que leurs pairs choisiraient de camoufler des produits défectueux ou pouvant comporter un danger, que les jeunes dirigeants imitent automatiquement les dirigeants plus chevronnés, éventuellement par souci de loyauté. Ce qui semble indiquer qu'un comportement moralement anormal devient de plus en plus la norme; à preuve, certaines pratiques, considérées généralement comme frauduleuses par la police, sont vues, par les entrepreneurs, comme de bonnes techniques commerciales, pures et simples.

Voici des exemples de ce genre de comportement: aux États-Unis, une société de construction d'avions a produit des milliers d'avions dont le réservoir à carburant défectueux a causé bon nombre de morts; cette société a prétexté que le problème était attribuable au fait que l'agence de surveillance hésitait à intervenir. Ou encore: pour une société minière, le problème était l'incidence sociale de l'obéissance à la loi, alors qu'il n'y avait qu'une alternative: exposer 150,000 consommateurs à l'eau polluée, ou exposer 32,000 employés à une mise à pied éventuelle.

L'indulgence avec laquelle les tribunaux traitent les criminels en col blanc et le genre de poursuites intentées contre ces criminels ont poussé certains à dire que le système de justice pénale doit être doté de moyens qui lui permettraient d'augmenter le nombre d'enquêtes et de poursuites intentées. De plus, on semble reconnaître qu'il faut réviser les lois actuelles, de façon à permettre des peines plus sévères. Des peines plus sévères réduiraient le nombre de récidivistes, en raison de la valeur dissuasive de la lutte contre la criminalité en col blanc. Même si la dissuasion n'a pas réussi à réduire la criminalité traditionnelle, elle a un rôle important à jouer dans la réduction de la criminalité en col blanc, étant donné le type de personnes dont il s'agit.

Dans le cas du criminel en col blanc, il s'agit d'une personne qui a été formée en fonction des normes de la société, car son accession à un poste de commande et de confiance en témoigne. Par conséquent, si le criminel doit faire face à la possibilité réelle d'être arrêté, poursuivi et démuné de ses titres, il sera plus susceptible d'être dissuadé d'adopter un comportement illégal. Penseur intelligent et prudent, il se rendra compte que, s'il est arrêté, il risque davantage que le criminel de la rue, auquel on est habitué. Par exemple, les poursuites contre les

[Text]

greater than the cost of apprehension to a traditional street criminal. For example, prosecution of white collar criminals in Australia, especially those violating the consumer protection provisions of the Trade Practices Act of 1974, has led to significant organizational improvements and the prevention of recidivism.

From a different perspective, a survey of losses incurred through fraud, waste and abuse in federal agencies in the U.S. indicated that most of them were operating vulnerable systems because of the inadequacy, the ineffectiveness, the neglect or the absence of internal controls. This study revealed that inadequate controls exposed millions of dollars to the risk of loss, theft and misuse. It was further noted that fraud in government institutions was frequently due to the absence of internal controls—the inadequacy of internal controls and the neglect of internal controls.

• 1005

What appears necessary is the recognition of the problem, and the development of a preventive or corrective strategy which is both applied and effective and which incorporates the view of the Solicitor General of Canada, the Hon. Robert Kaplan, who has invited businesses to take a more active policing role in the protection of company assets.

At this point I wish to introduce Mr. David Conway, who is the Manager of Resources Protection of Mitel Corporation. Mr. Conway will outline the proactive posture undertaken by the corporation to impact white collar crime specifically.

David.

Mr. David M. Conway (Manager, Resources Protection, Mitel Corporation): Members of the committee, we at Mitel Corporation have recognized that existing preventive approaches associated with combating white collar crime are mechanically oriented and rather reactive in nature. We believe that an act, once committed, indicates a failure on behalf of the resources protection personnel. Therefore our thrust is a proactive posture, where corporate vulnerability is greatly reduced through ongoing measurements and evaluation. The following diagram graphically represents our strategy.

What I will do at this point, if you do not mind, is just move and come back to the diagram later.

To ensure the effective operation of this approach, we recognize the need for highly skilled resources protection officers—skilled in business, law, criminology and human relations. To this end, we have instituted professional development programs for all departmental personnel. The key to combating white collar crime effectively is the responsibility of all personnel in their daily activities. Our resources protection personnel participate in an in-depth program with a three-month duration, and all company personnel are involved in sensitization programs on a regular basis.

[Translation]

criminels en col blanc, en Australie, surtout ceux qui ont enfreint les dispositions sur la protection du consommateur de la *Trade Practices Act* de 1974, ont donné lieu à d'importantes améliorations hiérarchiques et à l'éradication du récidivisme.

D'un autre point de vue, une enquête sur les pertes causées par la fraude, le gaspillage et les abus dans les organismes fédéraux, aux États-Unis, a révélé que la plupart d'entre eux exploitaient des systèmes vulnérables, étant donné que les contrôles internes étaient insuffisants, inefficaces, inexistantes, ou qu'on ne les appliquait pas. L'étude a démontré que des contrôles insuffisants laissaient des millions de dollars se perdre, être volés ou mal utilisés. En outre, on a signalé que la fraude, dans des institutions gouvernementales, était souvent attribuable à l'absence ou à l'insuffisance de contrôles internes, et au fait qu'on ne les appliquait pas.

Il faudrait reconnaître le problème et mettre au point une stratégie ferme et efficace, stratégie qui tienne compte de l'opinion du Solliciteur général, l'honorable Robert Kaplan, qui a invité les entreprises à s'intéresser de façon plus active à la protection des biens de la société.

A ce moment-ci, j'aimerais présenter M. David Conway, directeur du Service de protection des ressources de la société Mitel. M. Conway exposera les lignes de conduite adoptées par la société pour se protéger de la criminalité en col blanc.

David.

M. David M. Conway (directeur, protection des ressources, Mitel Corporation): Membres du Comité, nous, de la société Mitel, avons reconnu que les méthodes préventives prévues pour lutter contre la criminalité en col blanc relèvent plutôt de la mécanique, qu'elles ne s'adressent pas au problème proprement dit. Selon nous, si un acte est perpétré, c'est le personnel de la protection des ressources qui subit un échec. Par conséquent, notre ligne de conduite est préventive; la vulnérabilité de la société est sensiblement réduite, grâce à une évaluation et à des contrôles permanents. Le diagramme suivant vous explique notre stratégie.

A ce moment-ci, si vous êtes d'accord, je poursuivrai la lecture du texte, et je reviendrai un peu plus tard au diagramme.

L'efficacité de cette approche dépend, selon nous, d'agents de protection des ressources très compétents dans les domaines suivants: le commerce, le droit, la criminologie et les relations humaines. A cette fin, nous avons prévu des programmes de perfectionnement professionnel à l'intention de tout le personnel des services. Un des éléments clés de la lutte contre la criminalité en col blanc est le sens des responsabilités de tous les employés dans le cadre de leurs activités quotidiennes. Notre personnel de protection des ressources participe à un programme approfondi de trois mois, et tout le personnel de la société participe, de temps à autre, à des programmes de sensibilisation.

[Texte]

The key, we would suggest, to the reduction of corporate vulnerability, and as a consequence increased profitability, lies in the notion of culture. We have become a society driven by fear: the fear of failure, the fear of rejection by our own peers and superiors. At Mitel this position is not tolerated by senior management. All persons contribute; we are all Mitel Corporation. The Resources Protection Department is a service function which by design assists departments in their daily activities.

All security precautions in place are put into effect only after human factors have been considered and met. The result of this approach has been a reduction in personal losses by employees of 73.6% over the last two years.

Studies indicate, as Tony suggested, that large companies are more apt to fall victim to pilferage than government, and government more apt than small companies. We have identified the factors in place which facilitate this crime.

At Mitel Corporation all employees, including the chief executive officer and chairman of the board, are on a first-name basis, with an open-door policy. We do not allow the dehumanization of the business milieu, and hence avoid the faceless crime previously alluded to. We feel we have come upon a sincere methodology which reduces crime and have established its success at Mitel.

The Chairman: Thank you.

Mr. Beatty: Gentlemen, thank you very much for your presentation, which has been very helpful. Could I ask you to turn for a minute to the subject of the committee's hearings, which is computer crime per se? I think one of the very valid arguments you are making is that institutions have a responsibility themselves to do whatever they can to put proper safeguards in place to prevent themselves from becoming victims of computer crime. But could you comment on whether you feel there is any role which the law can play in assisting them?

Mr. Juliani: From the Mitel perspective, they have recognized the need that the corporation is responsible for protecting its own assets. Governments inject millions of dollars, for example, in high-tech. How much money has government invested in prevention? Maybe it should not. This should be, we believe, the responsibility of the individual corporation, as alluded to by the present Solicitor General. To what extent industry has heeded this warning, we are not sure. Mitel—and David can allude to this even further—have recognized this need. They have invested not just in thought but in actions, in prevention, in proactive strategies.

David, you might wish to comment specifically on this, on what is being done now at Mitel.

Mr. Conway: In contrast to most corporations, we have sat down and we have taken a look at the issue of computer crime. I think you will find most industry thinks in terms of hardware, thinks in terms of decoding, scrambling devices, etc.; and

[Traduction]

Il est essentiel, selon nous, d'atténuer la vulnérabilité de l'entreprise; il faut tenir compte à la fois de la rentabilité accrue et de la notion de culture. Nous sommes devenus une société mue par la peur: la peur de ne pas réussir, la peur d'être rejeté par nos pairs et nos supérieurs. A Mitel, la haute direction n'accepte pas cela. Tous les employés contribuent; la société Mitel, c'est tous les gens qui y travaillent. Le rôle du service de protection des ressources est d'aider les divers services dans leurs activités quotidiennes.

Toutes les mesures de sécurité n'entrent en vigueur qu'après qu'on a étudié l'aspect humain de chaque question. Ainsi, on a constaté que les pertes personnelles des employés ont baissé de 73.6 p. 100 au cours des deux dernières années.

Comme Tony l'a signalé, les études démontrent que les grandes sociétés sont plus susceptibles d'être victimes de chapardage que le gouvernement, et que le gouvernement est plus susceptible de l'être que les petites entreprises. Nous avons identifié les facteurs qui facilitent ce genre de crime.

A la société Mitel, tous les employés, y compris le président-directeur général et le président du conseil d'administration se tutoient; toutes les portes sont ouvertes. Nous ne permettons pas à notre milieu d'affaires de devenir déshumanisant et, par conséquent, nous écartons le crime imperceptible auquel on a fait allusion. Selon nous, nous avons mis au point une méthode réelle, qui réduit l'incidence du crime, et nous l'avons appliquée de façon réussie à la Mitel.

Le président: Merci.

M. Beatty: Messieurs, je vous remercie de votre allocution, qui a été très utile. Permettez-moi de parler un peu de l'ordre de renvoi du Comité, qui consiste à étudier les infractions relatives aux ordinateurs. Un de vos arguments très valables, me semble-t-il, veut que les institutions ont la responsabilité de faire ce qu'elles peuvent pour prévoir les sauvegardes appropriées, de sorte qu'elles ne seront pas victimes d'infractions relatives aux ordinateurs. Mais selon vous, la loi aurait-elle un rôle à jouer, un rôle qui consisterait à les aider?

M. Juliani: La Mitel a reconnu que c'est à elle de protéger ses propres biens. Le gouvernement affecte des millions de dollars à la haute technologie, par exemple. Mais quelle somme a été investie dans des mesures préventives? Il ne devrait peut-être pas le faire. Selon nous, cette responsabilité relève de chaque entreprise, comme l'a indiqué le Solliciteur général actuel. Nous ne savons pas au juste dans quelle mesure l'industrie a tenu compte de cet avertissement. A Mitel, nous l'avons fait; David pourra vous en dire plus long à ce sujet. La Mitel n'a pas simplement étudié la question, elle a également pris des mesures préventives, adopté des stratégies de prévention.

David, vous pouvez peut-être renchérir en nous disant exactement de quelles mesures il s'agit.

M. Conway: Contrairement à la plupart des sociétés, nous avons pris le temps d'étudier la question des infractions relatives aux ordinateurs. Dans l'industrie, on s'intéresse surtout au matériel, au décodage, aux mécanismes pour brouiller les communications, etc.; à ce moment-ci, il est

[Text]

it becomes significant at this point to think that anything that has been designed by man then too can be defeated by man.

If we at Mitel Corporation are going to address the issue of corporate vulnerability through computer crime, we must first identify the type of individual apt to perpetrate the deed and then examine the systems in that light.

• 1010

I make note here that systems audits in most corporations are the responsibility, usually, of the finance organization or accounting, whatever the case may be, and at Mitel the systems audits are conducted by the resources protection people. We look at the systems and we ascertain if there are inherent weaknesses in it that would tempt people. We take a look at the computers and we say: What type of person is apt to take the information access to the computer? We have come to the conclusion— or we believe, at any rate—that the majority of people who gain access to a computer and as a consequence perpetrate an evil doing, if you will, do so probably accidentally. Some fellows on the computer may be playing *Donkey—Kong* or something like this and he accidentally hits the wrong button; he now has accessed our finance system. As a consequence he now is in possession of knowledge. A life crisis in conjunction with this knowledge may very well be the ingredients that lead down the road of computer crime.

As a consequence we view our response to that to be, first, to ensure that the computer has all those basic well thought-out mechanisms in it that do not allow one key to access one system from another; secondly, and most importantly to us, we take a look at the individuals within the corporation. If we identify the life crisis which is usually the key, we impact that proactively rather than attempt to deal with the individual who has perpetrated the deed reactively.

Does it all make sense?

Mr. Beatty: I will read the transcript.

Mr. Juliani: If I could give a specific example: If someone is in need of money at Mitel. Think of last year with the interest rates being so high. A fellow has to renew his mortgage. It was at 12%; now it is 22%. What Mitel would do would be to loan the individual the money for that particular mortgage. You have a healthier, happier employee contributing to the company. There is no need to involve the criminal law. This is not a new approach. It has been done in Japan and in other countries as well. This is actively impacting the vulnerability of the individual; traditionally they could have waited and reacted and then involved the criminal law.

Mr. Beatty: I think it is certainly fair to argue that companies have a responsibility to have proper security measures around their systems and, further, that good employer-employee relationships are essential, not just from the point of

[Translation]

important de songer à ceci: tout ce qui a été conçu par l'homme peut également être démolé par l'homme.

Si nous, de la Mitel, devons nous attaquer au problème de la vulnérabilité de la société par rapport aux infractions relatives aux ordinateurs, nous devons d'abord préciser quel genre d'individu serait susceptible de commettre ce genre d'infraction; par la suite, il faut faire l'étude des systèmes, à la lumière des conclusions que nous aurons tirées.

Il faut dire ici que dans la majorité des sociétés, la vérification analytique relève habituellement du services des finances ou de la comptabilité; chez Mitel, les vérifications analytiques sont effectuées par les services de protection des ressources. Nous analysons les systèmes, pour déterminer si ceux-ci ont des lacunes qui pourraient tenter les gens. Nous étudions les ordinateurs, et nous demandons quel genre de personne est susceptible d'avoir accès à cet ordinateur. Nous en sommes venus à la conclusion, que nous croyons bonne, voulant que la majorité des gens qui ont accès à un ordinateur et qui, par conséquent, commettent une infraction, le font accidentellement. Un type peut jouer à *Donkey—Kong*, ou à un autre jeu informatique, et il touche le mauvais bouton; il peut avoir accès à notre système financier. Il a donc ces renseignements à sa disposition. Si une crise personnelle s'ajoute à cet accès accidentel aux renseignements, on peut se retrouver sur la voie des infractions informatiques.

En conséquence, nous pensons qu'il faut d'abord faire en sorte que l'ordinateur soit protégé par des mécanismes bien pensés, qui empêchent de passer d'un système à un autre en ne touchant qu'une seule commande; deuxièmement, et c'est ce qui importe dans notre société, nous sommes attentifs à nos employés. Si nous décelons une crise personnelle chez un de nos employés, ce qui donne habituellement lieu à des infractions, nous essayons de régler cette crise avant qu'il n'ait commis une infraction.

Vous me suivez?

M. Beatty: Je lirai la transcription.

M. Juliani: Permettez-moi de vous donner un exemple précis. Un employé de Mitel a besoin d'argent. L'année dernière, les taux d'intérêt étaient très élevés, et supposons qu'un employé ait eu à renouveler son hypothèque. Son taux antérieur était de 12 p. 100, et on lui demande 22 p. 100 maintenant. Chez Mitel, dans ce cas, nous prêtons de l'argent à cet employé. Ainsi, celui-ci est plus heureux et il travaille mieux. Il n'est pas nécessaire de faire intervenir le droit pénal. Notre méthode n'est pas nouvelle; elle a été appliquée au Japon et ailleurs. Nous rendons notre employé moins vulnérable, alors que traditionnellement, dans les autres entreprises, on attend, et on réagit après coup, pour faire intervenir le droit pénal.

M. Beatty: On peut certainement dire que les compagnies se doivent d'avoir des mesures de sécurité appropriées pour leurs ordinateurs et que de bonnes relations entre employeur et employé sont essentielles, non seulement du point de vue de la

[Texte]

security but from a point of view of productivity, and many other concerns as well, but it goes somewhat beyond the scope of this committee's work to look exclusively at that. Do you not feel that there is a role for the law to play as well? What if, having offered people low-interest loans, having had good relationships with them, having put proper security measures around your system, you find that somebody steals from Mitel. Is there not a role for the law to play?

Mr. Juliani: Yes, and this is why we eluded to the effect of deterrence in this area. The criminal law has definitely a role to play. Assuming all the intervention on the part of Mitel fails or any other company, then the question is that we have to go to the criminal law and the criminal law has to be very specific and we feel that deterrence does have a role; sanctions do have a role in this particular environment because you are dealing with someone who, as we have mentioned, has been habilitated. He has certain standards and norms. He is deviating from them. So he would be more likely to be affected by deterrence as opposed to the traditional offender who may never have been habilitated. But we have assumed that and then tried to rehabilitate someone who has never been habilitated in this particular sphere. I think the criminal has a role to play in effectively implementing deterrence perspectives in terms of the sanctions.

Mr. Conway: I think what is significant, however, and cannot go unnoticed, is that whatever the costs that would be incurred by the federal government, society, as the consequence of the introduction of a law, whatever the total bottom line of that would be, I am sure that we could far more successfully impact the problem if we thought more in terms of culture as a motherhood statement.

Mr. Beatty: Surely the two are not mutually exclusive. It would seem to me the same applies for bank robbery or employee fraud at any level. You have two ways of dealing with it. The first is at the social level, trying to reduce the desire of individuals to commit the offence. I guess there are really three of them. Second, an institution has a responsibility to have proper security; and third, where all else fails, there is the law. No one of those is enough in itself or obviates the need to act in the other areas.

Mr. Conway: I think what is significant there is, "when all else fails, then there is the law."

• 1015

Mr. Beatty: For example, would you feel in instances where, in the United States, there are publications that give information on how to break into specific computer systems, that all else has failed there; very slick, very professional publications, which have a high circulation?

Mr. Conway: Partially tongue in cheek, my response there would be that the type of person—we are talking profiling here—who is apt to play in a computer terminal has a certain mind-set; the type of person who gets into computing sciences has a certain mind-set. It is a fairly new sort of blend of personalities to Canadian society. I put it to you that for as many of these publications that hit the street that indicate to a

[Traduction]

sécurité, mais également pour ce qui est de la productivité, entre autres; mais nous nous éloignons de notre sujet d'étude. Ne pensez-vous pas que la loi ait un rôle à jouer? Supposons que vous avez offert à vos employés des prêts à intérêt peu élevé, que vous avez de bonnes relations avec eux, que vous avez doté vos systèmes informatiques de mesures de sécurité adéquates, qu'arrive-t-il si vous découvrez que quelqu'un vole encore Mitel? Ne pensez-vous pas que la loi a un rôle à jouer?

M. Juliani: Oui, et c'est pourquoi nous faisons allusion au rôle de dissuasion. Le droit pénal a certainement un rôle à jouer. En supposant que toutes les interventions de notre société, ou d'une autre, échouent, il faut recourir au droit pénal, qui a un rôle très précis, tout comme la dissuasion; les sanctions sont importantes dans ce milieu, parce que, comme nous le disons, on traite avec un employé qui a été autorisé. Il doit respecter certaines normes de conduite. Il est donc probable qu'il sera plus sensible aux moyens de dissuasion, alors que le criminel ordinaire l'est moins, n'ayant jamais été autorisé. Nous avons essayé d'autoriser à nouveau quelqu'un qui ne l'avait jamais été dans ce domaine. Je crois que le droit pénal a un rôle à jouer dans ce contexte de dissuasion par imposition de sanctions.

M. Conway: Dans ce contexte, il ne faut pas oublier que peu important les coûts que devra assumer le gouvernement fédéral, ou la société, à la suite de l'adoption d'une loi; quel que soit le coût, nous pourrions, j'en suis sûr, nous attaquer d'une façon beaucoup plus productive au problème en le faisant du point de vue de la culture, du point de vue social.

M. Beatty: Les deux ne s'excluent pas. Je crois que cela s'applique également aux vols de banque ou à des fraudes d'employés. Il y a deux façons de s'attaquer au problème. Premièrement, au niveau social, on peut essayer de réduire le désir de commettre des infractions. En fait, il y a trois moyens de s'attaquer au problème. Deuxièmement, les institutions doivent se doter de moyens de protection adéquats; troisièmement, au bout du compte, il y a la loi. Aucun de ces moyens ne suffit en soi à faire disparaître l'importance des autres.

M. Conway: Il est intéressant de souligner que vous avez dit: «au bout du compte, il y a la loi».

M. Beatty: Par exemple, aux États-Unis, certaines publications donnent des informations sur la façon d'accéder à certains systèmes d'ordinateurs; pensez-vous que toutes les autres solutions aient échoué dans ce cas? Il s'agit de publications excessivement professionnelles, très sophistiquées, et qui ont un vaste réseau de distribution.

M. Conway: On peut dire, et c'est une observation un peu ironique, que le genre de personne qui est susceptible de jouer avec un terminal d'ordinateur a une certaine configuration mentale; bref, les gens qui s'intéressent aux sciences de l'informatique ont une certaine démarche de l'esprit. C'est un type de personnalité assez nouveau dans la société canadienne. Je peux vous dire que beaucoup de gens trouvent parfaitement

[Text]

would-be perpetrator how to do it, there are as many people saying: Is that not fascinating? Now let us find some mechanism by which we can neutralize that access possibility. It has become the biggest game in town.

Mr. Beatty: Sure. Then there is a good living to be made from security measures as well. But the point is this: Presumably there is a clientele for those magazines who are utterly amoral as it relates to computer systems; they do not believe their standards of morality impede them from doing what they are doing. Is there not a role for the law to play in that instance?

Mr. Conway: I guess there would have to be.

Mr. Juliani: By "the law", do you mean in the reactive sense? What would you do? You would sanction the individual; you would hopefully, by affecting that individual, deter others. Again, this is the point: We do feel strongly that there is a role, as far as the criminal law is concerned, in this specific area of criminality that can be deterred, because you are dealing with people who understand the principle; you are not dealing with the traditional criminal, who has absolutely no indication of what you are trying to do with him. In this case, yes, you can be more severe. But it has to be consistent; your sanctions have to be consistent, there has to be a certainty aspect. There has to be certainty and severity, then you can be consistent. But if you start making exceptions for every individual because of his position, that erodes any effectiveness the criminal law might have.

Mr. Beatty: Tell me what nature of law you feel would be appropriate there. What is the best way to deal with this? One of the things we have been struggling with is whether we should have a computer bill, as such, which would give protection to software as opposed to operating from the copyright sense, possibly to say that manipulation of the data base that is unauthorized is an offence. Or possibly another option is to look at an offence akin to computer trespass, if you like, similar to physical trespass. Do any of those approaches seem appropriate to you, or do you feel that others would be more so?

Mr. Conway: It depends on what you are trying to impact. An individual could be accessing your computer system for the purpose of data crunching and not actually with the intention of writing a cheque or stealing proprietary information. If a law were to come into existence to attempt, somehow or other, to control the theft of CPU—central processing unit—time, you almost have to take a look at it in the perspective of computer trespass.

I put it to you that that is probably a greater cost to society in the long run. If someone is stealing information, the difficulty we have is that information is not seen to be property. If someone is accessing your mainframes off premises, there is sort of something kicking around. You can talk to them in terms of theft of telephone... communication—lines I guess. I do not think there is one law. I do not think one can talk in terms of one action to resolve what we would have to call a computer crime.

[Translation]

fascinantes les indications contenues dans ce genre de publications qui arrivent sur le marché. Maintenant, reste à trouver le moyen de neutraliser ces possibilités d'accès. C'est devenu le jeu le plus à la mode.

M. Beatty: Certainement. Mais j'imagine que l'on peut également gagner beaucoup d'argent à inventer des mesures de sécurité. Le problème n'en est pas moins qu'il doit y avoir une clientèle pour ces magazines parfaitement amoraux. Or, ces gens-là n'ont pas l'impression que leurs normes de moralité les empêchent de se conduire de cette façon. Est-ce que la loi n'aurait pas un rôle à jouer dans ce cas-là?

M. Conway: J'imagine que oui.

M. Juliani: Quand vous dites «la loi», qu'est-ce que vous envisagez exactement? Est-ce que vous pensez au remède possible? Pensez-vous que des sanctions contre certains individus seraient un facteur de dissuasion pour les autres? Cela nous ramène toujours au même problème: nous pensons que le droit criminel a un rôle à jouer, un rôle de dissuasion dans ce secteur particulier de la criminalité, car ce sont justement des gens qui comprennent les principes. Il ne s'agit pas des criminels traditionnels, qui n'ont aucune idée de ce que l'on essaie de faire. Dans ce cas, il est effectivement possible d'être plus sévère. Mais il faut également être logique. Les sanctions doivent être logiques, c'est un élément important. En plus d'être sévères, les sanctions doivent être certaines, c'est la seule façon d'être logique. Si, au contraire, vous commencez à faire des exceptions pour tout le monde à cause de la position sociale des intéressés, cela porte atteinte à l'efficacité du droit criminel.

M. Beatty: Quel genre de loi envisageriez-vous dans ce cas? Quelle est la meilleure méthode? Nous nous sommes demandé s'il fallait adopter un bill sur les ordinateurs axé sur l'aspect logiciel, et non pas sur l'aspect droits d'auteur. On pourrait, par exemple, partir du principe que la manipulation d'une base de données non autorisée est un délit. Il y a une autre possibilité, c'est de considérer que le délit est assimilable à une violation de propriété, une violation physique. Ces démarches vous semblent-elles appropriées, ou bien avez-vous d'autres idées?

M. Conway: Cela dépend de vos priorités. Vous pouvez considérer qu'une personne pénètre dans votre système d'ordinateur pour en modifier les données, et non pas dans l'intention d'écrire un chèque ou de voler des informations privées. Si l'on adoptait une loi pour contrôler les vols de temps d'utilisation d'unités centrales de traitement, il faudrait pratiquement considérer cela comme une violation d'ordinateur.

A mon sens, à long terme, les coûts, pour la société, risquent d'être encore plus élevés. Dans le cas de vol d'informations, le problème est que, jusqu'à présent, l'information n'est pas considérée comme une propriété. Si quelqu'un accède à votre unité centrale à partir de l'extérieur, cela fait, en quelque sorte, du remue-ménage. Vous pouvez leur parler de vol de lignes téléphoniques, de communications, si l'on peut dire. Je ne crois pas qu'il y ait une loi unique. Je ne pense pas que l'on

[Texte]

Mr. Beatty: If someone is using your computer to write cheques, that is fraud, as the law stands today, so that is dealt with by the law and there is no need for the committee to deal with that as such.

Theft of service, at the present time, is not an offence, nor is the information stored on a computer protected either. I suppose what we could do would be simply to amend the Code to include information under the definition of property, but it has philosophical and legal implications that are well beyond, I think, Parliament's ability at this point to grapple with, because you would have to get as well into control of other information stored in a manual form. I am not sure that at this point there is any consensus in society as to exactly what sort of control society would want to have over information if it were property.

• 1020

Mr. Conway: If I may go back to my original contention, you are right; the implications are incredible. The key might well be to place the onus of responsibility on the owner of the computer; if the individual is going to be negligent, and he is going to have the computer system function within his organization but that computer system lends itself readily to all kinds of access, then he in fact may even be the negligent party.

Mr. Beatty: To an extent, the market will correct that itself. But let me again draw an analogy to manually stored information. Presumably you have some manual records in your office, and presumably you have an obligation to have proper security. If an individual chooses to break into your office, there is a number of offences he may have committed: trespass, break and enter and possibly theft. The same would not apply if the information were held in a computer which had an on-line access capability. My concern is essentially to bring into the treatment of computerized information provisions somewhat parallel to what we have for manually stored information. In no way does the law of trespass release you from your obligation to have proper security around your office; you still have that obligation. But the fact that you may have been negligent, or that somebody may have been smarter than you, does not obviate the need for trespass law either.

Mr. Conway: Mind you, the existence of that law has become significant to the conversation—the existence of the law, hence its inclusion in assorted codes, hence the burden on the police department to enforce it—yet that law is so seldom used.

Mr. Beatty: I am sorry, the law is so seldom used for what?

[Traduction]

puisse, par une mesure unique, résoudre ce que nous sommes forcés d'appeler un crime informatique.

M. Beatty: Si quelqu'un utilise votre ordinateur pour écrire des chèques, c'est de la fraude; la loi actuelle prévoit déjà cela, et par conséquent, le Comité n'a pas vraiment besoin de s'en occuper.

A l'heure actuelle, le vol de services n'est pas considéré comme un délit, pas plus que le vol d'informations entreposées dans un ordinateur. J'imagine que l'on pourrait se contenter de modifier le code, pour ajouter l'information à la définition de la propriété, mais cela aurait des implications philosophiques et juridiques qui dépassent actuellement la portée d'une simple commission parlementaire. En effet, il faudrait également s'occuper du contrôle d'autres formes d'information, en particulier l'entreposage manuel des informations. Je doute que la société sache à l'heure actuelle quelle position elle souhaite adopter face au problème de l'information considérée comme une propriété.

M. Conway: Permettez-moi de revenir à mes premières observations, vous avez raison, les implications sont incalculables. La solution serait peut-être de charger le propriétaire de l'ordinateur de toute la responsabilité. S'il y a négligence, c'est-à-dire si l'ordinateur de son organisation est ouvert à toutes sortes d'abus, il sera considéré comme la partie négligente.

M. Beatty: Dans une certaine mesure, le marché rectifiera de lui-même. Mais permettez-moi de faire une analogie avec les informations entreposées manuellement. J'imagine que dans votre bureau vous devez avoir des dossiers, et vous devez également vous sentir obligé de les protéger. Si un individu décide de pénétrer par effraction dans votre bureau, il risque de commettre un certain nombre de délits: violation de la propriété, effraction, et peut-être vol. Dans le cas d'un ordinateur auquel peuvent être connectés en direct des terminaux d'accès, ces circonstances ne s'appliquent pas. Il me semble que nous devons chercher à protéger les informations sur ordinateur par des mesures en quelque sorte comparables aux mesures de protection des informations entreposées manuellement. Les dispositions de la loi portant sur la violation de propriété ne vous libèrent pas de l'obligation d'assurer la sécurité de votre bureau. Mais ce n'est pas parce que vous avez été coupable de négligence ou parce que quelqu'un a été plus malin que vous qu'une loi sur la violation de la propriété devient inutile.

M. Conway: Remarquez à quel point ce type de loi a pris de l'importance dans notre conversation. De tout cela on peut déduire que cette loi qui figure dans différents codes et qui charge les services de police d'un certain fardeau d'application est tout de même très rarement invoquée.

M. Beatty: Pardon, pour quelle raison la loi est-elle rarement invoquée?

[Text]

Mr. Conway: I cannot recollect that I have ever known anyone to be charged under the Trespass Act. I am sure people have, but I just cannot think of it.

I guess our concern today is that if a law comes into existence the intention is to view the possibility of introducing laws for the purpose of instituting controls, more regulations, and that is a reactive thing and does not do anything to resolve the problem. In the deterrence theory . . . where Tony points out that an habilitated person is more apt to be affected by the concepts of deterrence—it is almost universally accepted that the deterrence value of an act will only last six to eight months, whatever the case may be, and then it is gone and forgotten. So the law itself will not deter, I do not think. I do not believe it, at any rate.

If you want to impact the problem, and you want to think in terms of legislation, then you have to think in terms of getting the people who have a proprietary interest to take the necessary steps to ensure that the act is not committed, rather than put an act on the books so that if something is committed you can deal with it.

Mr. Beatty: I will come back to the institutions, but I want to pursue this point about the deterrent value of the law. Do you have pay TV in your house at the present time?

Mr. Conway: No, and I also have access to a convertor but do not use it.

Mr. Beatty: Why not?

Mr. Conway: Because it is against the law.

Mr. Beatty: Because it is against the law. Then surely there is some deterrent value in the law.

Mr. Conway: Are you asking me if I have ever committed a crime?

Mr. Beatty: No, I am asking you to confirm what you have just said, which is . . .

Mr. Conway: No. In the instance of pay TV . . .

Mr. Beatty: You do not use the convertor because it is against the law.

Mr. Conway: To be perfectly honest with you, I also happen to have a preprogrammed television set that it does not work on. But if you want to broaden the question and ask me if I have ever committed a crime because I knew that the Criminal Code existed for the purpose of deterring me, I would take the fifth.

Mr. Beatty: You are in the wrong country for that. Nor do I believe does the protection of the Canada Evidence Act apply to parliamentary committees.

Mr. Conway: I bow to your superior knowledge on the subject.

If deterrence were a significant factor, why is Mr. Kaplan concerned about finding mechanisms by which we can get more and more people out of penitentiaries? I do not believe that deterrence is significant.

[Translation]

M. Conway: Je ne me souviens pas d'avoir jamais entendu parler d'une personne accusée de violation de propriété. Cela a dû arriver, mais je ne vois pas d'exemple.

Aujourd'hui, nous nous disons que si une loi est adoptée elle aura pour but de mettre en place des contrôles, des règlements, ce qui constitue une mesure de réaction et ne résout pas vraiment le problème. On reconnaît généralement que l'efficacité de la théorie de dissuasion ne durait que six ou huit mois, après quoi tout est oublié. Cela dit, Tony a observé que plus une personne était compétente, plus elle risquait d'être sensible aux principes de la dissuasion. Dans ces conditions, la loi ne saurait jouer un rôle de dissuasion, du moins ce n'est pas mon opinion.

Si vous voulez attaquer le problème, vous allez devoir penser à légiférer d'une part, mais également penser au moyen d'intéresser les propriétaires d'informations, les gens qui sont le plus directement intéressés, aux mesures de prévention possibles. Cela vaudra beaucoup mieux que d'adopter une loi qui n'interviendra qu'une fois le mal fait.

M. Beatty: Je reviendrai tout à l'heure aux institutions, mais je veux parler tout de suite de l'élément de dissuasion de la loi. J'imagine que vous devez avoir la télévision payante chez vous?

M. Conway: Non, j'ai également un convertisseur que je n'utilise pas.

M. Beatty: Pourquoi pas?

M. Conway: Parce que c'est illégal.

M. Beatty: Parce que c'est illégal. Dans ces conditions, la loi comporte sûrement un élément de dissuasion.

M. Conway: Me demandez-vous si j'ai jamais perpétré un crime?

M. Beatty: Non, je vous demande de confirmer ce que vous venez de dire, c'est-à-dire . . .

M. Conway: Non. Dans le cas de la télévision payante . . .

M. Beatty: Vous n'utilisez pas le convertisseur parce que c'est illégal.

M. Conway: Pour être parfaitement honnête, je dois vous signaler que mon poste de télévision étant préprogrammé, il n'est pas compatible avec le convertisseur. Cela dit, si vous voulez élargir la question et me demander si j'ai déjà commis un crime en toute connaissance du Code criminel qui est là pour me dissuader, il faudrait que j'invoque le 5^{ème} amendement.

M. Beatty: Vous vous trompez de pays. Cela dit, je ne crois pas que les dispositions de la Loi sur la preuve au Canada s'appliquent aux comités parlementaires.

M. Conway: Je suis certain que vous connaissez ce sujet mieux que moi.

Si la dissuasion était un facteur déterminant, comme se fait-il que M. Kaplan soit à la recherche de mécanismes qui permettent de vider le plus possible les pénitenciers? A mon avis, la dissuasion n'est pas un élément déterminant.

[Texte]

• 1025

Mr. Beatty: Deterrence is surely significant. There are two issues here, perhaps, that are being confused. The first is one of whether there is any value in deterrence, whether deterrence works at all. The other is whether it is absolutely effective. No one would presume that it is absolutely effective. Otherwise we would not have murders taking place in Canada, nor would we have bank robbery or arson, if deterrence were 100% effective. One cannot argue back from that, saying: There is murder; therefore, the Criminal Code provisions as they relate to murder are totally ineffective and it would be ridiculous to have them in the Code, and that we should decriminalize murder.

Mr. Conway: Are you going to play history on the gentleman?

Mr. Juliani: If I may interject, this is a point that Dave and I disagree on. Deterrence does work. We have three groups in society. The first is the group that would not commit an offence because of their upbringing. There is a second group in society which most of us are part of. We do not commit the offence because of possible consequences. That is deterrence. There is a third group in society, which is a minor group, which will commit an offence regardless. So we are dealing here in deterrence with the larger group in society. So the criminal law does have a role to play in deterring this larger group, which is the middle group.

Mr. Beatty: And I would argue that in deterrence there are two separate grounds. One is the possibility of being caught, the second is the fact that society has said formally that something is wrong. There are many people who would not break the law, more out of concern that they were doing something which was morally wrong than out of a concern for being caught. Deterrence would act in both instances.

Mr. Juliani: Right.

Mr. Beatty: Going back to institutions—and I certainly agree with you that institutions have often been lax in terms of the security standards which they have around their systems and also in terms of their employee relations and so on—would you propose the government should legislate security standards or do you believe the market will correct itself?

Mr. Conway: The market will not correct itself in high technology, because the speed by which a project is conceived, developed, re-developed, marketed, re-developed, marketed is of such that yesterday's news is old news. My answer would have to be that the government should consider legislating the corporations in specific areas.

Just let me throw this out for what it is worth. In 1971, there were 41,000 peace officers in Canada and approximately 51,000 security guards. In 1981, there are 46,000 peace

[Traduction]

M. Beatty: Je suis sûr que la dissuasion est importante. D'ailleurs, il y a deux choses en cause, et nous les confondons peut-être. Pour commencer, il faut nous demander si la dissuasion a une valeur quelconque, si elle fonctionne le moins. Ensuite, il faut nous demander si son efficacité est absolue. Personne ne prétendra que son efficacité est absolue. Si c'était le cas, il n'y aurait pas de meurtres au Canada, il n'y aurait pas de vols de banques ou d'incendies volontaires, si la dissuasion avait une efficacité absolue. Cela dit, on ne peut pas non plus en déduire que puisqu'il y a des meurtres, c'est que les dispositions du Code criminel n'ont absolument aucune efficacité. On ne peut pas en déduire que les dispositions sur le meurtre du Code criminel sont parfaitement ridicules et qu'il faut décriminaliser le meurtre.

M. Conway: Vous voulez faire un peu d'histoire à monsieur?

M. Juliani: Vous permettez? C'est un sujet sur lequel Dave et moi-même ne sommes pas d'accords. J'estime que la dissuasion fonctionne. Dans la société, il y a trois groupes d'individus. Un premier groupe qui ne commet pas de délit parce que c'est comme cela qu'il a été élevé. Un second groupe de la société, dont la plupart d'entre nous faisons partie, qui ne commet pas de délit à cause des conséquences possibles. Ça, c'est la dissuasion. Vient ensuite un troisième groupe de la société, une minorité, qui commet des délits quelles qu'en soient les conséquences. Par conséquent, le facteur de dissuasion s'adresse au groupe le plus important de la société. Ainsi, le droit criminel joue un rôle déterminant pour ce groupe qui est entre les deux autres et qui est le plus important.

M. Beatty: À mon avis, la dissuasion fonctionne de deux façons: d'une part par la possibilité d'être pris, d'autre part du fait que la société a énoncé clairement que c'était mal. Beaucoup de gens hésiteront à contrevenir à la loi, pas tellement de crainte d'être pris, mais plutôt de crainte de faire quelque chose qui soit moralement répréhensible. La dissuasion fonctionne de deux façons.

M. Juliani: Parfaitement.

M. Beatty: Je reviens aux institutions. Je suis parfaitement d'accord avec vous quand vous dites que les institutions ont souvent été négligentes et n'ont pas toujours adopté les normes de sécurité qui auraient pu protéger leurs systèmes. Elles n'ont pas toujours non plus pris les mesures qui s'imposaient vis-à-vis de leurs employés. Pensez-vous que le gouvernement devrait imposer des normes de sécurité ou bien croyez-vous que la situation se rectifiera d'elle-même?

M. Conway: Le secteur privé ne corrigera pas lui-même la situation dans le domaine de la haute technologie à cause de la rapidité d'évolution d'un projet, de sa conception à son développement, son redéveloppement, sa mise en marché, son redéveloppement, sa remise en marché, etc. Ce qui est nouveau aujourd'hui sera vieux demain. Autrement dit, il y a place pour une législation des sociétés dans certains secteurs spécifiques.

Je vais vous donner un exemple; à vous d'en juger la valeur. En 1971, il y avait au Canada 41,000 agents de la paix et environ 51,000 gardes de sécurité. En 1981, il y avait 46,000

[Text]

officers in Canada and approximately 81,000 security guards. This would lead me to believe that people are concerned about what they are losing. The corporations are concerned about what they are losing and do not really know what to do about it. So they hire more security guards, more security guards, more security guards. The introduction of a law is just another law. It is just another one of the 300,000 or more laws. If the corporation cannot, if we cannot start thinking in terms of who are these security guards, who are the peace officers, how are they trained, what can they do, are they in a position to possess knowledge, then . . . The ultimate irony is watching someone walk through the front door of a high tech company and have the security officer spot him and ask him if he can take a look at what is in the envelope. The guy produces a schematic that is way beyond my ability to understand, as the chief of security for Mitel, and the security guard makes a judgment call and off the guy goes. The introduction of a law will not resolve our problem, our societal problem. The crimes will go on, because we do not have the mechanism in place to do anything about it. The corporations are making efforts, otherwise the force of security guards would not be growing at that rate, but there is nothing out there in terms of training, there is nothing out there in terms of direction.

Mr. Beatty: Society should be imposing no standards on institutions themselves.

Mr. Conway: Did you say no standards?

Mr. Beatty: Of security.

Mr. Conway: I would say society should be imposing standards on the institutions.

Mr. Beatty: How? I am sorry, I thought you were arguing that there should not be a law to do that. The question is how, then, does society at large do that except by resort to marketplace, if you cannot use the law?

Mr. Conway: All right. I am questioning the introduction of a law under the Criminal Code. I am suggesting that a publicly owned corporation has a responsibility to the shareholders; therefore, as surely as there is legislation compelling us to report our earnings, etc., that there should be actions taken compelling industry to maintain certain standards of resource protection.

• 1030

Mr. Juliani: On a more micro level, the industry should be compelled, possibly through a law, to set minimum standards.

Mr. Beatty: How would you determine those standards, particularly with the fact that, as you point out, the technology is very fast moving and it would be very difficult to incorporate into the law standards which would be valid by the time the law was proclaimed? It also presumes, I suppose, a degree of omniscience on the part of the government at the time when the law is passed that government is in fact current with the potential failings in systems.

[Translation]

agents de la paix au Canada et environ 81,000 gardes de sécurité. Cela semblerait prouver que les gens s'inquiètent de ce qu'ils perdent. Les sociétés s'inquiètent des pertes qu'elles constatent, sans très bien savoir quoi faire. Leur premier mouvement est d'engager des gardes de sécurité plus nombreux, de plus en plus nombreux. Une nouvelle loi, après tout, ça n'est qu'une autre loi. C'est une loi parmi 300,000 autres. Si le secteur privé, si l'ensemble de la société n'en vient pas à se demander qui sont ces gardes de sécurité, qui sont ces agents de la paix, comment ils sont formés, ce qu'ils peuvent faire, quelles sont leurs connaissances, dans ce cas . . . Finalement, le plus ironique, c'est de voir un garde de sécurité arrêter une personne qui entre dans un immeuble qui abrite une société de haute technologie et qui lui demande de lui montrer le contenu de son enveloppe. L'individu montre un schéma que moi-même, qui suis chef de la sécurité à Mitel, je ne comprendrais pas du tout et pourtant, le garde de sécurité prend une décision rapide et laisse l'individu partir. Ce n'est pas une loi qui résoudra notre problème, un problème pour l'ensemble de la société. Les crimes continueront, parce que nous n'avons pas les moyens d'y mettre fin. L'industrie privée fait des efforts; si elle n'en faisait pas, les gardes de sécurité ne se multiplieraient pas à ce rythme-là, mais rien n'est fait dans les secteurs de la formation, aucune orientation majeure n'est adoptée.

M. Beatty: La société ne devrait pas imposer de normes aux institutions.

M. Conway: Vous avez dit pas de normes?

M. Beatty: De sécurité.

M. Conway: Au contraire, c'est la société qui devrait imposer des normes aux institutions.

M. Beatty: Comment? Excusez-moi, je croyais vous avoir entendu dire qu'il ne fallait pas adopter de loi dans ce sens. Dans ces conditions, comment l'ensemble de la société peut-elle s'y prendre, sinon en laissant jouer les lois de la libre entreprise?

M. Conway: Attendez, ce que je conteste, c'est l'efficacité d'une loi dans le cadre du Code criminel. À mon sens, une société publique a des responsabilités envers ses actionnaires et par conséquent, aussi vrai que nous sommes forcés par la loi de déclarer nos gains, l'industrie privée devrait être forcée d'assurer certaines normes pour la protection des ressources.

M. Juliani: L'industrie devrait être obligée, éventuellement par voie législative, à fixer des normes minimales.

M. Beatty: Étant donné l'évolution très rapide de cette technologie, comment proposeriez-vous de fixer ces normes afin que la loi ne soit pas désuète avant même d'entrer en vigueur? Cela sous-entend également que le gouvernement est parfaitement au courant des carences éventuelles du système.

[Texte]

Mr. Juliani: The industry receives millions of dollars from government in terms of development. Every time Mitel puts up a building there are a lot of dollars coming in from the public purse. There are some controls in terms of that relationship; what controls are there in terms of protecting those assets? As part of the contract, for example, there is a security clause that protects the public assets that go into a corporation like that. Could it not be part of the contractual agreement that those assets must be protected via an established security department which has minimum standards in terms of qualifications of its personnel?

Mr. Conway: An example would be a government contract tendered—a defence contract, for example. There are standards required before that contract can be accepted. An interesting mechanism might be to make it part and parcel of what is required on the date of incorporation.

Mr. Beatty: Your suggestion would be that in instances where people are recipients of contracts or grants from the government you might attach a string to it but no other provisions would be written into the law for other institutions which would not be covered by that.

Mr. Conway: No, I suggest that, as one possibility for monitoring, that possibly on the date of corporation, the date of registration of a company, the company then recognize that it has a responsibility to society.

I guess I am kind of hung up on the notion that you cannot commit a crime if it is not there to be committed and that building penitentiaries and hiring police officers and that sort of stuff becomes somewhat reactive. Not that I do not have the utmost respect for the police, but do you know what I mean? If the person leaves his house open—I was teasing the lady on the committee here before we got started . . . and leaves his keys in his car, then he is inviting trespassing, inviting theft of his personal property and certainly inviting theft of his vehicle. The individual who perpetrates it could easily be a first-time offender. It could have been an impulse. This is a criminal person?

If we are going to impact the issue, be it computer crime, white collar crime, whatever crime in general, then the individual, the victim, has to have a responsibility.

Mr. Beatty: I do not think there is any difficulty with that. You are not arguing that we should decriminalize other offences such as theft from a house or theft of a car with someone's keys in it, are you?

Mr. Conway: I think you could look at a dual charge, yes.

Mr. Beatty: This is going somewhat beyond the scope of the committee's . . . You are just looking at principles.

Mr. Conway: Yes, I think you could look at a dual charge there. I think if a public company has its computers accessed and information is stolen then there might well be a responsibility on the part of the company as well as the thief.

Mr. Beatty: And if you have a chair on your front porch and somebody steals it, if it was not chained down then you could be charged yourself?

[Traduction]

M. Juliani: Le gouvernement verse des millions de dollars à ce secteur pour le développement. Chaque nouvelle usine construite par Mitel est en partie subventionnée par les deniers de l'État. Pour protéger ces investissements, les contrats contiennent une clause garantissant l'apport de l'État. Pourrait-on également prévoir une clause instituant un service de sécurité doté d'un personnel dûment qualifié?

M. Conway: À titre d'exemple, on pourrait prendre les contrats de fourniture du ministère de la Défense, contrats qui prévoient certaines normes. On pourrait donc exiger que ces normes deviennent obligatoires dès la constitution de la société.

M. Beatty: Vous voulez dire que seules les sociétés ayant des contrats de fourniture au gouvernement ou obtenant des subventions du gouvernement seraient assujetties à ce genre de normes.

M. Conway: Non, ce n'est pas ce que je voulais dire; c'est au moment de la constitution d'une entreprise que celle-ci reconnaîtrait officiellement ses responsabilités vis-à-vis de la société.

La plupart des criminels, à mon avis, le deviennent à cause des tentations et ce n'est pas en construisant des prisons et en engageant des agents de police qu'on extirpera le mal. On encourage les voleurs en ne fermant pas les portes à clef ou en laissant les clés de contact sur les voitures. La facilité même de l'entreprise pousse au crime ceux qui n'avaient pas de casier judiciaire, mais qu'on ne saurait pourtant classer parmi les criminels.

Afin de lutter contre la truanderie, la criminalité des cols blancs et la criminalité en général, c'est la victime éventuelle qui doit elle aussi assumer sa responsabilité.

M. Beatty: Vous ne voudriez quand même pas décriminaliser les vols commis dans des maisons dont les portes n'ont pas été fermées à clé ou de voitures dont les clés de contact n'ont pas été enlevées?

M. Conway: Les deux parties devraient peut-être être inculpées.

M. Beatty: Je crois que cela dépasse quelque peu notre mandat.

M. Conway: Oui, les deux devraient peut-être être inculpées. Lorsque des renseignements sont volés dans le service informatique d'une société d'État, la société elle-même ainsi que le voleur devraient être tenus pour responsables.

M. Beatty: Si l'on vole une chaise de votre perron sans que celle-ci ait été boulonnée au plancher, il faudrait que vous soyez donc vous aussi inculpé?

[Text]

Mr. Conway: You are right. We are beyond the scope of the question. We are discussing the computer crime element, if the company has a responsibility. To answer that question, if the person put a chair on their front porch and their chair was stolen and they were too stupid to bring it inside, yes, one might make the case for the fact that there was a dual responsibility for the theft of the chair.

Mr. Beatty: Or if a child's bicycle was stolen and it was not chained down or locked in the basement the child would be responsible?

Mr. Conway: We train our children from the day they are born as a good society.

Mr. Beatty: Could I ask just about one other area, and that is the third-party protection? Professor David Flaherty from the University of Western Ontario argued that the legislation should go well further than that which we contemplated. I think he would like to deal with the issue of privacy somewhat through the back door here. His argument is—and I think it is a valid one—that institutions which hold information about you or about me have a responsibility to us to ensure the security of that information—for example, an insurance company which might have our medical records; another company which might have credit information, a bank, for example, which would have information relating to our finances. Is there any merit in writing provisions into the law, either into the civil law or into criminal law, to impose standards for data security upon institutions which hold information about other parties?

• 1035

Mr. Conway: That is exactly what I was talking about, yes.

Mr. Beatty: I gathered at the time what you were referring to was an institution's responsibility to itself and its shareholders to protect its own system. I am talking here about third parties as opposed to . . .

Mr. Conway: Let us expand and say the institution's responsibility to society to ensure that. I can relate this to Mitel. Our personnel records, payroll records, medical records, etc., are kept on one machine; and the machine is very, very, very closely guarded, because there is a recognition that this is the most sensitive of all information in terms of the individual. Yes, I definitely believe . . . what do you think, Tony?—there should be some kind of mechanism demanding of them levels of security and responsibility surrounding that information.

Mr. Beatty: Should an individual whose privacy is violated have recourse to seek damages in some way?

Mr. Juliani: Privacy is difficult. We were talking about an individual working within a company, who voluntarily gave his information. I am having a problem with this in terms of how much protection should the company be required to give to this individual. I am assuming he is an employee. He voluntarily gave this information, did he not?

Mr. Beatty: Let us use a different example of my medical records, which may be held by a life insurance company. I

[Translation]

M. Conway: Oui. Nous nous écartons peut-être effectivement de notre sujet. Il est question notamment de la mesure dont une société victime de la truanderie est elle-même responsable dans une certaine mesure. Si on oublie de rentrer une chaise qui se trouvait sur le perron et que cette chaise est ensuite volée, le propriétaire est en quelque sorte partiellement responsable du vol.

M. Beatty: Et un enfant qui laisserait traîner son vélo serait donc responsable en cas de vol?

M. Conway: Nous devons éduquer nos enfants dès leur jeune âge.

M. Beatty: Je voudrais vous poser une question concernant la protection de tiers. Le professeur David Flaherty de l'université de Western Ontario faisait valoir que la loi devrait aller bien plus loin que ce qui n'a été envisagé. La question de la protection de la vie privée est devenue quelque peu secondaire dans ce contexte. D'après le professeur Flaherty, les institutions qui détiennent des renseignements concernant les particuliers doivent veiller à les protéger; par exemple, les compagnies d'assurance qui conservent des dossiers médicaux ou les banques qui possèdent des renseignements concernant les cotes de crédit et l'état financier de leurs clients. Pensez-vous qu'il soit utile d'inclure des dispositions dans les Lois civiles ou criminelles imposant des normes de sécurité aux institutions afin de garantir le secret des données qu'elles détiennent au sujet de tiers?

M. Conway: Oui. C'est justement cela ce dont je parlais.

M. Beatty: Vous sembliez parler plus tôt des responsabilités des institutions pour se défendre elles-mêmes ainsi que leurs actionnaires alors que moi je pense plutôt aux tiers.

M. Conway: On pourrait parler de la responsabilité des institutions vis-à-vis la société toute entière. Ainsi chez Mitel, des dossiers du personnel, de la paie, des dossiers médicaux etc., se trouvent tous dans un ordinateur qui est extrêmement bien protégé, car il s'agit de renseignements qui touchent à la vie privée des particuliers. Il faudrait donc prévoir des normes de sécurité pour protéger ces renseignements.

M. Beatty: Les particuliers dont les dossiers auraient été divulgués devraient-ils pouvoir obtenir des dédommagements?

M. Juliani: C'est une question difficile. Nous parlions d'une personne travaillant pour une entreprise et qui fournit ce renseignement volontairement. Dans quelle mesure l'entreprise devrait-elle garantir le secret de ces informations à l'employé en question?

M. Beatty: Prenons l'exemple de dossiers médicaux détenus par une compagnie d'assurance. Le dossier médical doit être communiqué pour obtenir une police d'assurance.

[Texte]

voluntarily gave my medical records as a precondition of getting insurance.

Mr. Juliani: Yes.

Mr. Beatty: If I had my druthers, I would rather not give my medical records. Do you not feel there is potential damage to me if that information is given out or if financial information is given out by a bank improperly, relating to me as an individual?

Mr. Juliani: Are you not doing a disservice to the bank who is not privy to that information? The bank gives you a mortgage, and for some reason, God should recall you from this earth. Are you not doing a disservice to the bank, which is not privy to that information?

Mr. Beatty: No, I am sorry. My argument is this. For example, take your financial records that a bank has already.

Mr. Juliani: Right.

Mr. Beatty: No one argues that the bank should not have those records.

Mr. Juliani: Financial records.

Mr. Beatty: Yes. You have agreed they obviously have your bank statement; they could not function otherwise. It does not mean other groups either have an entitlement to that information or that it is appropriate that they should have it. What if, through lax security standards, those people got access to your bank records or information relating to your finances? Should you have some recourse against the bank, which has maintained lax standards; or should your only recourse be through the courts, presumably against the individual who violated the institution?

Mr. Juliani: I have two minds on that, and this is where the problem comes in. I cannot give you a specific answer because I can see both sides. Someone maintaining minimum standards established by law is one thing, but I am looking at it from the point of view of a bank which would like to have your medical records. They are financial institutions but would like to have your medical records in order for them to make a determination on you as a potential client. They want that information; it is necessary for them. Are we going to say: No, you are not allowed to have that information, because the third party or the fourth party will be prosecuted?

Mr. Beatty: No, I am sorry.

Mr. Juliani: So there are two . . .

Mr. Beatty: My question may have been unclear. My argument is not that, where informed consent exists, an institution should not be able to get information about an individual. Indeed, when you apply for a credit card, for example, you sign a release which allows your bank to turn over information to the credit card company. That is no difficulty. You may very well sign a release at the time you apply for insurance to allow the insurance company to have access to your medical records which your doctor has. That is no difficulty; there is informed consent.

[Traduction]

M. Juliani: Oui.

M. Beatty: Les gens préféreraient bien entendu ne pas devoir communiquer leurs dossiers médicaux. Lorsque des renseignements médicaux ou financiers concernant un particulier sont communiqués à des tiers par ces institutions, le particulier en question risque de subir des préjudices, vous ne trouvez-vous pas?

M. Juliani: Mais on pourrait tout aussi bien dire que la banque risque de subir un préjudice si elle n'est pas mise au courant de certains faits concernant la santé d'une personne à laquelle elle consent un prêt hypothécaire.

M. Beatty: Ce n'est pas ce que je voulais dire. Prenons les dossiers financiers détenus par une banque.

M. Juliani: Oui.

M. Beatty: Il est tout à fait normal que les banques possèdent ce type de dossiers.

M. Juliani: Oui.

M. Beatty: Lorsqu'on a un compte en banque, il est tout à fait normal que la banque connaisse l'état de votre compte, autrement cela ne marcherait pas. Mais cela ne veut pas dire pour autant que ces renseignements devraient normalement être communiqués à d'autres. Qu'est-ce qui arrive si par suite de mauvaises mesures de sécurité, une autre institution obtient des renseignements concernant votre compte en banque ou votre état de finance? En pareil cas, devrait-on pouvoir poursuivre la banque elle-même ou bien uniquement l'employé coupable?

M. Juliani: Il y a du pour et du contre des deux côtés. Il y a d'une part l'obligation faite aux sociétés d'assurer des normes de protection minimums de leurs dossiers; mais d'autre part, il y a les banques qui aimeraient avoir accès aux dossiers médicaux de leurs clients pour se faire une meilleure idée de la mesure dans laquelle elles peuvent leur accorder un crédit. Vous voudriez qu'on interdise de communiquer ces dossiers par crainte de poursuites?

M. Beatty: Non, ce n'est pas ce que je voulais dire.

M. Juliani: Donc . . .

M. Beatty: Je me suis sans doute mal exprimé. Une institution devrait pouvoir obtenir des renseignements sur un particulier avec l'accord de celui-ci. Ainsi lorsqu'on fait une demande pour obtenir une carte de crédit, on autorise en même temps la banque à communiquer certains renseignements à la société de crédit. Cela va de soi. De même lorsqu'on souscrit une police d'assurance, on autorise la compagnie d'assurance à demander le dossier médical au médecin traitant.

[Text]

The problem comes where those institutions then have the information. Where they were holding it to themselves for their own purposes, you had no quarrel with that at all; but they have maintained lax security, for example, around their computer, and some unauthorized person—unauthorized either by the bank or by you—gets access to that information, violates your privacy and possibly gains information which could be damaging about you. Should you have recourse for damages against the institution that was holding the information...

• 1040

Mr. Juliani: You are talking about negligence. Lack of security would be negligence, obviously, in that particular case. Possibly some recourse. I have difficulty with that. I cannot give you a specific: "Yes, you do have recourse."

Mr. Conway: I would have to say absolutely. If the bank has possession of certain confidential personal information and for some reason, as a consequence of their negligence or lack of security, that information was to fall into the hands of someone who would... I think you might want to make a point here that, as in the case of slander or libel, there has to be some demonstrated damage to the individual as a consequence of this information being out; that yes, they should be held equally responsible.

Mr. Beatty: Could I just pursue that one point further? It may not be possible to establish there was financial damage to you by an invasion of your privacy, but it may very well be that you choose to hold some information yourself. Establishing damages there would be very difficult, but there could be embarrassment to you and you could be very resentful of the fact that someone has gained information about you improperly. A case in point would be, for example, if you were in the United States and you were subscribing to some of the cable TV services there in the U.S. as opposed to Canada, some of which were, for example, pornographic services, and the cable company did not maintain proper standards of security on its records, and someone else found that and then perhaps subsequently used that for a mailing list to send you materials that you found offensive, or the information were to get out and was found to be embarrassing to you, although no commercial damage as such to you but is an invasion of your privacy. In that instance, would you feel the cable company should be in any way libel?

Mr. Conway: I would think yes. The key, I would think, is that there is an up-front understanding that the information that you are surrendering is either that you choose it to be treated as confidential or you do not care. The onus thing comes back on the consumer. If he chooses not to make clear to the supplier that the information is confidential, then if it becomes public it is less of a problem. If the individual chooses to indicate possibly in a box on the end of it that he does not want this information made public, then the onus of responsibility lies on the individual in possession to ensure that the person's wishes are adhered to; the individual should be held accountable for something—I do not know if I could guess at

[Translation]

Donc, lorsque des sociétés détiennent des renseignements avec le consentement des particuliers, cela ne pose pas de problème. Mais si, à cause de mesures de sécurité insuffisantes dans le service d'ordinateur, une personne, mandatée ni par la banque ni par vous, parvient à soustraire des renseignements qui risquent de vous porter préjudice, devriez-vous pouvoir intenter des poursuites contre l'institution détenant ces renseignements à votre sujet?

M. Juliani: Dans ce cas, ce serait de la négligence et il y aurait peut-être moyen d'avoir recours devant les tribunaux. Mais je ne suis pas sûr.

M. Conway: Je pense que cela ne fait aucun doute. Si une banque détient des renseignements confidentiels concernant une personne et que par suite de négligence, ces renseignements tombent entre les mains d'un tiers, des poursuites devraient pouvoir être intentées. Tout comme pour les poursuites en diffamation, il faut que la divulgation de ces informations ait porté préjudice à l'intéressé, auquel cas les banques seraient tenues pour responsables.

M. Beatty: Il peut être extrêmement difficile pour une personne d'établir qu'elle a subi un préjudice financier, alors que le fait que certains renseignements à son sujet ont été divulgués peut l'avoir sérieusement embarrassée. Prenons le cas d'une personne qui s'abonne à une société cablôvision américaine pour capter des émissions pornographiques, fait qu'un tiers parviendrait à apprendre et dont il se servirait pour envoyer à la personne en question du matériel qu'elle jugerait choquant, ou bien encore que le fait de s'être abonnée aux émissions pornographiques deviendrait connu et que, sans causer de préjudice matériel, cela serait néanmoins embarrassant. En pareil cas, la compagnie de cablôvision devrait-elle être poursuivie pour diffamation?

M. Conway: Je pense que oui. Il s'agit de s'entendre au départ si les renseignements que l'on fournit sont ou non confidentiels. C'est au client de s'en assurer. Si le client ne précise pas qu'il fournit certains renseignements sous garantie de secret, il ne peut pas ensuite s'en plaindre si ces renseignements sont divulgués. Si par contre une personne précise clairement que les renseignements fournis doivent rester confidentiels, il incombe à la société d'en assurer le secret et elle sera éventuellement tenue pour responsable si les renseignements étaient divulgués. Mais en principe, je ne m'en fais pas pour les sociétés de cablôvision.

[Texte]

what—for releasing that information. The cable company would be the least of all concerns.

My mind starts to move in the direction of doctors who begin to computerize medical records on IBM home computers and that sort of stuff and, because they want access to the Toronto Stock Exchange, put a communicator on it and now there is potential two-way communication. The possibilities would be terrible.

Mr. Beatty: Yes. One other example, perhaps a more mundane example, would be that of credit card companies again. They quite properly have access to information about how you have used your credit card, what purchases you have made and so on. You do not quarrel with their right to have that, but it is nobody else's business, however. There is no injury to you in terms of economic damage to you in somebody else getting that information but it is an invasion of your privacy. Now if there is lax security on the part of the credit card company, should you have any recourse against them? You think that you should.

Mr. Conway: I would think yes.

Mr. Beatty: Irrespective of whether there has been financial damage to you?

Mr. Conway: I think of one of the criminological theories of labelling, and I think of information being even more dangerous to the individual being put in the hands of someone else who may choose to interpret it and the significant consequence. Can you imagine, for example, someone who went to an extremely traditional orthodox church who used their credit card to buy a subscription to *Playboy*, or whatever the case may be?

• 1045

There is a labelling process; an absolute labelling process. As a consequence, where there are no monetary laws, the loss to the individual and his community is incredible.

Mr. Juliani: Just a point on this—and I come back to it—how far do you go? The doctor has your information. For safe keeping, he passes it on to IBM. Is the doctor liable for that information having been released, in terms of your privacy, or is it the IBM company? Is the doctor in turn going to sue IBM, which is keeping that information? How far do you go in this?

Mr. Beatty: It may be that as a condition of contract with IBM you may want to put that on. The difficulty that an individual has is that an individual's relationship with a large institution is sufficiently one-sided that it is very difficult for the individual to dictate conditions. For example, in the case of a credit card company I am not sure the banks are all that interested in your desire to dictate conditions to them at date of security. If you were to put a rider on the bottom of your application for a credit card, they would tell you they were not terribly interested in your business; and they have all the leverage there.

[Traduction]

Je vois plutôt un danger du côté des médecins qui mettent les dossiers de leurs patients sur ordinateur et qui ensuite utilisent ce même ordinateur pour communiquer en duplex avec la bourse de Toronto, ce qui pourrait donner lieu à des fuites terribles.

M. Beatty: En effet. Prenons encore l'exemple des sociétés qui distribuent les cartes de crédit. Ces sociétés possèdent bien entendu les renseignements sur la façon dont les cartes de crédit sont utilisées et sur les achats effectués par leurs clients. Cependant ces renseignements ne devraient pas tomber entre les mains de tiers, car cela serait une atteinte à la vie privée des intéressés même si cela n'entraîne aucun dommage matériel pour eux. Si à cause de a société de crédit, une fuite se produit, le client devrait-il pouvoir avoir recours contre la société?

M. Conway: Je pense que oui.

M. Beatty: Même si le client n'a pas subi de préjudice financier?

M. Conway: Les renseignements ainsi divulgués risquent, dans certains cas, de ruiner la réputation des intéressés. Prenons, par exemple, le cas d'une personne membre d'une Église très orthodoxe qui utiliserait sa carte de crédit pour s'abonner à *Playboy*, fait qui deviendrait ensuite connu des membres de la congrégation.

C'est comme une «dénunciation»; le gars est marqué au fer rouge. En conséquence, lorsqu'il n'y a aucune législation portant compensation monétaire, la perte pour la personne en question et sa communauté est absolument incroyable.

M. Juliani: Un petit retour en arrière: jusqu'où doit-on aller? Le médecin a des renseignements sur vous. Pour les garder en sécurité, il les remet à IBM. Le docteur est-il responsable, pour ce qui est de votre vie privée, si ces renseignements sont publiés ou serait-ce plutôt la compagnie IBM? Le médecin va-t-il, à son tour, poursuivre IBM qui a la garde de ces renseignements? Jusqu'où va-t-on?

M. Beatty: Il se pourrait qu'une des conditions du contrat passé avec IBM précise ce genre de chose. Le problème du particulier, c'est que la relation qui existe entre lui et une grosse institution est plutôt déséquilibrée et il est très difficile au particulier de dicter ses conditions. Par exemple, dans le cas d'une compagnie qui émet des cartes de crédit, je ne suis pas sûr que les banques sont vraiment intéressées à ce que vous leur imposiez vos conditions quant à la sécurité. Si vous deviez ajouter un avenant au bas de votre demande de carte de crédit, la compagnie vous ferait poliment savoir qu'elle n'est pas vraiment intéressée à faire affaires avec vous; c'est la compagnie qui a le gros bout du bâton.

[Text]

In the case you cited of a doctor perhaps going into a service contract with another company, my guess is that his bargaining position would be much better. The only instance where I could see the law—and again, I argued with Professor Flaherty, who rejects my contention that it is going beyond the scope of this committee's work—but the only instance where I could see the law coming in is where individuals are availing themselves of widely used services and where they have very little leverage relative to the institution; where there is no market correction, in essence.

Mr. Conway: A friend of mine wished a Steinberg's cheque-cashing card. This was after the Constitution had just come into play and everybody was feeling quite righteous about it.

Mr. Beatty: They demanded his SIN, among other things.

Mr. Conway: He would not put his SIN down, he would not put his credit history down, but he wrote on the bottom of the form: I have a Loblaw's cheque-cashing card; should you choose not to offer me one, the question will be why. On the strength of his name, his home address and his telephone number, he was granted a cheque-cashing card.

I am not sure the consumer does not have the leverage to place riders on credit card companies. They are in the business of doing business; and it is the choice of the consumer. Because they are in the business of doing business, they very probably would want to restrict the information.

Mr. Beatty: No doubt, no doubt. I do not argue that credit card companies do not have protections on their lists. But I would invite you, the next time you renew your VISA card, to write a letter to VISA saying you want assurances from them that they are prepared to sign a contract with you personally, holding themselves liable for any invasions of your privacy that result from lack of security standards. Then let us know what response you get from VISA.

Mr. Conway: It is just my style.

Mr. Beatty: Thank you very much, gentlemen.

Thank you, Madam Chairman.

The Chairman: Thank you, Mr. Beatty.

Maybe I will ask a small question of Mr. Conway.

What is your background? I am curious. Your title is Manager of Resources Protection. Do you have a background in criminology also?

Mr. Conway: I am a social worker. That will blow my story. Most people employed in security in Canada have a background either in policing company facilities or in military

[Translation]

Dans le cas du médecin que vous avez cité, où il y a un contrat de service avec une autre compagnie, j'ai l'impression que sa force de négociation serait de loin meilleure. Le seul cas où la loi, à mon avis... Encore une fois, j'en ai discuté avec le professeur Flaherty qui rejette mon hypothèse que cela déborde des cadres des travaux de votre Comité... Mais le seul cas, dis-je, où il me semble que la loi pourrait avoir un effet, c'est celui où des personnes souscrivent à des services offerts à une vaste clientèle et où l'individu a très peu de poids par rapport à l'institution; essentiellement, où les forces du marché n'agissent pas.

M. Conway: Un ami désirait se procurer une carte pour encaisser ses chèques chez Steinberg. C'était à l'époque où la Constitution venait tout juste d'être adoptée et tout un chacun était à cheval sur les principes.

M. Beatty: On a exigé d'avoir son numéro d'assurance sociale, entre autres choses.

M. Conway: Il n'a pas voulu donner son numéro d'assurance sociale, il ne voulait pas donner les renseignements relatifs à son crédit, mais il mit au bas de la formule: je tiens une carte semblable de Loblaw; si vous décidez de ne pas m'en offrir une, je voudrai savoir pourquoi. Sur la foi de son nom, de son adresse et de son numéro de téléphone, on lui accorda cette fameuse carte qui lui permit d'encaisser ses chèques au magasin.

Je ne suis pas sûr que le consommateur n'a pas le poids voulu pour placer un avenant au bas de la formule des compagnies de carte de crédit. Ces compagnies sont là pour faire des affaires; le choix en revient au consommateur. Parce que ces compagnies veulent brasser des affaires, elles décideraient fort probablement de restreindre l'accès à ces renseignements.

M. Beatty: Sans doute, sans doute. Je ne dis pas que ces sociétés de crédit ne protègent pas leurs listes. Cependant, je vous inviterais, la prochaine fois que vous renouvelerez votre carte VISA, d'écrire une lettre à la compagnie VISA pour lui dire que vous voulez qu'elle vous assure qu'elle est prête à signer un contrat avec vous personnellement, se rendant responsable pour toute invasion de votre vie privée qui serait le résultat d'un manque de mesures de sécurité de sa part. Vous nous ferez alors savoir la réponse que vous obtiendrez de VISA.

M. Conway: C'est en plein mon genre.

M. Beatty: Merci beaucoup, monsieur.

Merci, madame le président.

Le président: Merci, monsieur Beatty.

J'aimerais peut-être poser une petite question à M. Conway.

Quels sont vos antécédents? Je suis curieuse. Votre titre est celui de directeur de la protection des ressources. Avez-vous aussi des antécédents en criminologie?

M. Conway: Je suis travailleur social. Et voilà ma réputation qui s'envole. La plupart des gens qui oeuvrent dans le domaine de la sécurité au Canada viennent soit d'une force policière

[Texte]

service. My background is in social work, community animation.

The Chairman: I had the impression that you had a special background. I think it was very interesting, the perspective you gave us this morning, and also the dynamism of your corporation. I think even working with people from the Department of Criminology shows avant-garde in corporation management and so on. I feel it is a bit unusual, but I just felt it was worth mentioning, because many more corporations certainly could use the talent of people in sciences like criminology in the preventive aspect. I think you called it positively acting...

I think we have dealt a lot more with the behaviour of the employees and the possibility of committing an infraction than with the technology itself. I do not know if you are familiar, Mr. Conway, with the product that your company is producing. I have the impression—but please just correct me—that technology is growing so fast. But I was wondering if it was a preoccupation of Mitel to include in its new concept of technology the security mechanism in the first place. I mean, every time you conceive of a new hardware piece or software program, do you have that preoccupation first?

• 1050

Mr. Conway: The product which comes immediately to mind is something called the SX2000, which is our niftiest, newest mechanism that is going into the marketplace. There is built into it, from a software and from a hardware perspective, safety packages on that entire telephone switching piece of equipment.

The Chairman: And is it part of the regular item you are selling, or is it added cost?

Mr. Conway: Part and parcel of the item we are selling as it is. We have just produced a desk top telephone we call "Contact", and programmed right into the permanent memory of the machine are lockout devices, security devices, etc.

The Chairman: So the customer does not have to pay a special fee over and above cost just to make sure that he has the appropriate security?

Mr. Conway: It is part of the package, yes.

The Chairman: It is part of it. I must say, since I love criminology, I was very impressed by your approach in categorizing society as to those who will commit crime. Especially in the computer business, I was always tempted to say that cheating the system for the fun of cheating the system is more or less the crime that is appealing to people who have the brains to commit that kind of crime.

[Traduction]

d'une autre compagnie, soit des forces militaires. Moi, je faisais du travail social, de l'animation communautaire.

Le président: J'avais l'impression que vos antécédents étaient différents. Je crois que c'est très intéressant, cette perspective dont vous nous avez fait part ce matin ainsi que le dynamisme de votre société. Je crois que travailler avec des spécialistes issus d'une faculté de criminologie prouve l'avant-gardisme de la gestion de la compagnie et ainsi de suite. Je crois que c'est un peu inhabituel, mais j'ai cru que cela valait la peine d'être souligné parce que plus de sociétés pourraient certainement faire bon usage du talent de gens qui ont étudié des sciences comme la criminologie, surtout pour ce qui est de l'aspect de la prévention. Je crois que vous appelez cela de l'action positive...

Je crois que nous avons beaucoup plus traité du comportement des employés et des possibilités qu'ils ont de commettre des infractions, plutôt que de traiter de la technologie elle-même. Je ne sais pas si vous connaissez très bien, monsieur Conway, le matériel que produit votre société. J'ai l'impression, mais vous me direz si je fais erreur, que la technologie avance à pas de géant. Mais je me demandais si c'était là une préoccupation de Mitel que d'inclure dans son nouveau concept de la technologie les mécanismes de sécurité dès le départ. Autrement dit, toutes les fois que vous mettez en branle un nouveau projet de matériel ou de logiciel, est-ce là votre première préoccupation?

M. Conway: Le premier produit à me sauter à l'esprit est quelque chose que l'on appelle le SX2000, qui est notre plus beau petit nouveau bijou de mécanisme que nous commercialisons. Et pour le matériel et pour le logiciel, il y a toute une gamme de mesures de sécurité qui font partie intégrante de cette pièce d'équipement qui achemine les appels téléphoniques.

Le président: Et ces mesures font-elles partie de cet article que vous vendez, ou les ajoute-t-on pour un prix additionnel?

M. Conway: Ces mesures de sécurité font partie intégrante de cette pièce d'équipement que nous vendons telle quelle. Nous venons tout juste de sortir un téléphone qui va sur le dessus de n'importe quel bureau et que nous appelons «Contact»; on a inséré dans la mémoire permanente de cet appareil toutes sortes de mécanismes d'interdiction d'accès, de sécurité et que sais-je encore.

Le président: Donc, le client n'a pas besoin de payer un supplément pour jouir d'une sécurité adéquate?

M. Conway: Ces mesures font partie intégrante du système, oui.

Le président: Elles en font partie. Je dois dire, puisque j'aime bien la criminologie, que votre façon de diviser la société en catégories pour ceux qui commettront des crimes m'a vraiment emballée, surtout pour ce qui est du domaine de l'ordinateur, j'ai toujours été tentée de dire que tricher le système par pur plaisir est plus ou moins le genre de crime qui

[Text]

But as for society, I saw in your brief that it is cleaner to commit a crime with a computer and, probably, the morality or immorality of that kind of crime is evaluated in a different pattern. That is why, probably, we have not taken any special action towards these crimes. They might be evaluated in terms of . . . For instance, if you go to a corner store and somebody is stealing \$200 with a gun, to society in general it appears to be a very bad crime; yet, somebody could steal \$200,000 with just new technology and it does not appear to carry exactly the same connotation of immorality.

Mr. Conway: You may be interested to know that the American Society for Industrial Security reckons that the average computer crime perpetrated in the United States is \$1 million.

The Chairman: So that is the size of it. But can you explain, Dr. Juliani, why in general people tend to evaluate or attach that concept of crime to a very small amount of money, because it is perpetrated in not a nice manner and I would say by those who do not have the intelligence of committing it otherwise, while they are actually very lenient and not necessarily very preoccupied with, nor are they making any march on the Hill to prevent the other crimes which are much more sophisticated.

Mr. Juliani: The blood and gore associated with traditional street crime is something that we are exposed to every day. But I maintain that the more damaging aspect is this lack of morality—the decline in morality which exists in white collar crime, computer crime, call it what you will. The issue of what is fraud is no longer that it is fraud but that it is good business practice. It is this type of decline of traditionally acceptable behaviour. And now it has become in terms of unethical behaviour as being more and more acceptable. It is something that society does not accept as being severe. Personally I believe the decline in morality which is associated with this type of activity is much more damaging than that with a bank robber, for example, at the individual level.

Take, for example, the manager or the senior executive who defrauds a corporation. Look at what he is doing in terms of an example. In two studies we cited, managers are becoming more and more accepted in terms of their behaviour and their subordinates, obviously. Why? Because they are looking at net profit. Is it criminal to cheat on your expense account, \$1,000, when that \$1,000 was directly involved in terms of obtaining a contract? In the corporation that is rather acceptable, is it not? He has contributed to the final goal. But from the morality perspective it is rather damaging, and it is this type of build-up that I think is much more damaging than any street criminal . . .

[Translation]

est l'apanage de ces gens qui ont l'intelligence voulue pour commettre ce genre de crime.

Quant à la société elle-même, j'ai vu dans votre mémoire que cela fait plus propre de commettre un crime en se servant de l'ordinateur et que, probablement, la moralité ou l'immoralité de ce genre de crime s'évalue de façon différente. C'est pourquoi, probablement, nous n'avons pas pris de mesure spéciale pour ce genre de crimes. On pourrait les évaluer en termes de . . . Par exemple, si vous allez à l'épicerie du coin et que quelqu'un vole \$200 à la pointe du fusil, la société en général semble considérer qu'il s'agit là d'un crime très sérieux; cependant, quelqu'un pourrait voler \$200,000 grâce à cette nouvelle technologie, mais on ne semble pas y attacher la même notion d'immoralité.

M. Conway: Vous serez peut-être intéressé d'apprendre que *The American Society for Industrial Security* (la Société américaine de sûreté industrielle) a calculé que le crime moyen commis grâce à l'ordinateur aux États-Unis «rapporte» 1 million de dollars.

Le président: Voilà où nous en sommes. Cependant, pourriez-vous nous expliquer, monsieur Juliani, pourquoi les gens, en général, ont tendance à prendre très au sérieux le vol d'une très petite somme d'argent parce que le vol est perpétré sans gentillesse aucune et, je dirais, par ceux qui n'ont pas l'intelligence de commettre le crime autrement, tandis que cette même société est toujours très indulgente à l'égard de ces crimes plus sophistiqués; elle ne s'en préoccupe pas nécessairement beaucoup ni ne fait jamais de démonstration sur la Colline parlementaire pour les empêcher.

M. Juliani: Le sang et la violence que l'on associe au crime traditionnel sont des choses qui nous guettent tous les jours. Cependant, je crois que l'aspect le plus dommageable de tout cela, c'est ce manque de moralité . . . ce déclin de moralité que l'on associe au crime chez les cols blancs, au crime commis par ordinateur, appelez cela comme vous voulez. Il ne s'agit plus de savoir si l'on commet une fraude, il s'agit plutôt de savoir si la fraude commise s'accepte en affaires. Voilà le genre de déchéance qui dégrade le comportement que l'on trouvait traditionnellement acceptable. Question d'éthique, ce comportement devient de plus en plus acceptable. La société trouve que ce n'est pas vraiment très grave. Personnellement, je crois que cette déchéance de moralité publique que l'on associe à ce genre d'activité est beaucoup plus dangereuse que celle que l'on retrouve chez le voleur de banque, par exemple, au niveau individuel.

Par exemple, prenez un directeur ou un cadre qui fraude une compagnie. Regardez l'exemple qu'il donne. Dans deux études que nous avons citées, les subordonnés acceptent de plus en plus ce genre de conduite de la part des gestionnaires, de toute évidence. Pourquoi? Parce que l'on ne voit que le profit net. Est-ce criminel de tricher sur votre note de frais pour \$1,000 quand ce \$1,000 a directement servi à décrocher un contrat? Du point de vue de la compagnie, c'est plutôt acceptable, n'est-ce pas? Après tout, c'est ainsi que l'on a réussi à atteindre le but fixé. Mais du point de vue de la moralité, c'est plutôt dommageable et c'est ce genre de pourrissement qui me semble

[Texte]

• 1055

The Chairman: That is why we are confronted with a choice.

✓ **Mr. Juliani:** —and we have to act.

The Chairman: Which law do we touch and how do we deal with computer crime? The Criminal Code usually has much more a connotation of morality than does other administrative law. If we had a computer law per se, creating an offence, but an offence that—I do not pretend if I do not make a stop I commit a crime, commit an infraction. I think that is the dilemma we are in. I know the deterrence . . . I agree with you; to a certain point, there are some people whose reputations would certainly be damaged by a criminal record and who would certainly not have that kind of thing because of their record. There are others who would, for a profit, as long as they were not caught. The day they are caught, they are usually very repentant; but before that, they continued to operate.

That is the choice we have to make. Or do we have a mix of both, enforcing the Criminal Code with regard to computer crime along with your dual-responsibility approach? I feel that is certainly interesting in terms of also putting the onus on the one who is helping in the perpetration of the crime. I have the feeling that certainly, when you contribute to it by your own negligence, as you were saying before . . .

Mr. Conway: To make the point on deterrence, in the little Dave Conway test group here, 59 poor souls appeared in my office in the last 365 days guilty of some horrible deed—from stealing a telephone to God knows what. What was interesting was that the first question I asked of the 59 people, as the security officer, was: What have you done? It is the social worker in me; I cannot resist it. The answer is always: I took. I allow a pause; then I say: You mean you stole. You can just see the expression on the individual's face change. They have already rationalized the action. I guess part of my contention is that simply introducing a law . . . Give mankind time, they will rationalize their way around it. If we are to impact the problem, we have to take it one step before that.

The Chairman: Thank you for your contribution. I think it is certainly a very original perspective. It will be taken into account, and we thank you very much for appearing before us. I apologize for being late in coming from Montreal this morning.

[Traduction]

beaucoup plus dangereux que tout ce que peut faire un criminel ordinaire . . .

Le président: Voilà pourquoi nous devons faire un choix.

M. Juliani: . . . et il nous faut agir.

Le président: Quelle loi devons-nous modifier et que faisons-nous pour ces crimes que l'on commet par ordinateur? Le Code criminel implique une certaine moralité beaucoup plus que toute autre législation administrative. Si nous devons adopter une Loi sur les ordinateurs, comme telle, créant une infraction, mais une infraction qui . . . je ne prétends pas que si je ne fais pas . . . on efface et on recommence . . . je commets un crime, je commets une infraction. Je crois que c'est là le dilemme que nous avons. Je connais les mesures dissuasives . . . Je suis d'accord avec vous; jusqu'à un certain point, il y a certaines personnes dont les réputations seraient certainement entachées par un casier judiciaire et qui ne feraient certainement pas ce genre de chose à cause de la crainte d'un tel casier. Il y en a d'autres qui le feraient allégrement, pour le profit, tant et aussi longtemps qu'on ne les y prend pas. Le jour où ils sont pris, ils font habituellement preuve d'un très grand repentir, avant ce jour fatidique, cependant, ils vont bonnement leur petit chemin.

Voilà le choix que nous avons à faire. Ou devrions-nous avoir un judicieux mélange des deux, c'est-à-dire assurer l'application du Code criminel pour ce qui est du crime commis par ordinateur tout en utilisant votre méthode de double responsabilité? Je crois que c'est très intéressant parce que celui qui aide à perpétrer le crime a aussi sa part de responsabilités. Je crois vraiment que lorsqu'il est plus facile de commettre un crime à cause de votre négligence, comme vous le disiez plus tôt . . .

M. Conway: Tout simplement pour mieux illustrer cette dissuasion, dans le petit groupe témoin Dave Conway, 59 pauvres âmes ont été entraînées dans mon bureau pendant ces 365 derniers jours coupables de crimes absolument horripilants . . . ça allait du vol d'un téléphone à Dieu sait quoi encore. Ce qui est intéressant, c'est que la première question que j'ai posée à ces 59 personnes en ma qualité de responsable de la sécurité, était: «Qu'avez-vous fait?» C'est le travailleur social qui revient à la surface; il m'est impossible d'y résister. La réponse est toujours: j'ai pris. Et s'ensuit une pause; ensuite je dis: «Vous voulez dire que vous avez volé.» C'est alors comme on dit, que la face leur tombe. Les coupables ont déjà justifié leur geste. Autrement dit, pour moi, simplement adopter une nouvelle loi . . . Fiez-vous à l'homme: encore un peu de temps il se sera bien trouvé une bonne raison pour contourner la loi. Si nous voulons résoudre le problème, il nous faut agir avant d'en être arrivé à cette étape.

Le président: Merci pour votre apport. Je crois que votre perspective est très originale. Nous en tiendrons compte et nous vous remercions beaucoup d'avoir pris la peine de vous déranger. Je vous présente mes excuses si je suis arrivée en retard de Montréal, ce matin.

[Text]

The committee will resume its work on Wednesday, May 18, at 3.30 p.m. in Room 306. The meeting is adjourned.

[Translation]

Le Comité reprendra ses travaux le mercredi 18 mai, 15h30, salle 306. La séance est levée.



*If undelivered, return COVER ONLY to
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9*

*En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9*

WITNESSES—TÉMOINS

Mr. Dave M. Conway, Manager, Resources Protection, Mitel Corporation, Kanata, Ontario;

Professor Tony J. Juliani, Department of Criminology, Ottawa University.

M. Dave M. Conway, Gérant, Protection des ressources, Mitel Corporation, Kanata, Ontario;

Professeur Tony J. Juliani, Département de Criminologie, Université d'Ottawa.

HOUSE OF COMMONS

CHAMBRE DES COMMUNES

8.9.10
14.15.10

Issue No. 9

Fascicule n° 9

Wednesday, May 18, 1983

Le mercredi 18 mai 1983

Chairman: Céline Hervieux-Payette

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

*Procès-verbaux et témoignages
du Sous-comité sur*

Computer Crime

Les infractions relatives aux ordinateurs

of the Standing Committee on Justice and Legal Affairs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

CONCERNANT:

Matters pertaining to the Order of Reference

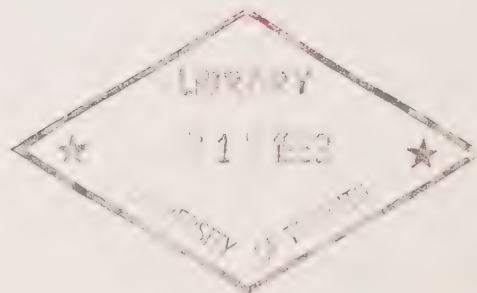
Questions relatives à l'ordre de renvoi

WITNESSES:

TÉMOINS:

(See back cover)

(Voir à l'endos)



First Session of the

Première session de la

Thirty-second Parliament, 1980-81-82-83

trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, MAY 18, 1983
(11)

[Text]

The Sub-committee on computer crime met this day at 3:40 o'clock p.m., the Chairman Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Céline Hervieux-Payette.

Designated Alternates Members presents: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: Professor Grant Hammond, Counsel, Law Center, University of Alberta, Edmonton, Alberta and Mr. George E. Fisk, Barrister, Gowling and Henderson, Ottawa, Ontario.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements and answered questions.

At 5:33 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 18 MAI 1983
(11)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h40, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Céline Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etibocoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: Professeur Grant Hammond, avocat, Centre d'études juridiques, Université d'Alberta, Edmonton, Alberta et Me George E. Fisk, avocat, «Gowling and Henderson», Ottawa, Ontario.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations et répondent aux questions.

A 17h33, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Wednesday, May 18, 1983

• 1541

Le président: La séance du Sous-comité sur les infractions relatives aux ordinateurs est ouverte. Aujourd'hui nous entendrons le professeur Grant Hammond de l'Université de l'Alberta, d'Edmonton, et M. George Fisk, avocat d'Ottawa.

I would like to ask Professor Hammond to make his statement. We will proceed with questions after the two witnesses have given their presentations.

Welcome to Ottawa.

Mr. Grant Hammond (Law Center, University of Alberta): Thank you very much indeed. Perhaps I should first introduce myself. I then want to explain something about documentation, if I may, after that.

First of all, the strange accent hails originally from New Zealand; I practised law for some years in the largest firm there. I had some connection with firms in the technology and broadcasting sector, which is where my interest in this topic first came from. Subsequently, I worked in the United States on IBM's behalf and taught at various American universities before going to Dalhousie Law School in Canada. I am currently counsel to the Institute of Law Research and Reform at the University of Alberta.

During the time I have been in Canada, I have undertaken several reports for federal departments, particularly in the area of broadcasting policy, telecommunications policy, and subsequently this matter.

How I came to be involved may be of some interest to the committee. The Department of Justice, partly as a result of some material I had written, asked if I could assist them with a background paper on some aspects of computer crime. Because, in effect, I am a civil servant who, amongst other things, has to advise the Alberta government on these matters, I had to ask permission of my institute to give me a certain amount of release time, which they agreed to do, partly because there is some interest in the provinces in this topic also and the problem of overlapping jurisdiction and matters of that kind.

It may also interest you to know, by way of background, that computer crime is not just of interest to high technology firms in central Canada. I can perhaps indicate that there have been some problems in the oil patch, where seismic computerized information is also a matter of some concern and there has been litigation there.

The department made it possible for me to go back to the United States and to visit with certain law firms there that specialize in these areas, and also to visit with Professor Richard Dole, who has drafted some of the U.S. legislation in this particular area. The department further made it possible for me to attend the CIPS Conference, which enabled some consultation with industry also.

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mercredi 18 mai 1983

The Chairman: I declare open this meeting of the Subcommittee on Computer Crime. We are happy to have with us today Professor Grant Hammond of the University of Alberta, Edmonton, as well as Mr. George Fisk, Counsellor in Ottawa.

Je demanderais au professeur Hammond de faire sa déclaration d'abord. Nous allons entendre les déclarations des deux témoins avant de poser nos questions.

Bienvenue à Ottawa.

M. Grant Hammond (centre du droit, Université de l'Alberta): Merci beaucoup. Je me présente d'abord. J'expliquerai ensuite un point au sujet de la documentation.

D'abord, l'accent étrange vient de la Nouvelle-Zélande. J'ai fait partie de la plus grande étude d'avocats pendant un certain nombre d'années. J'ai été appelé à y travailler avec des sociétés de technologie et de radiodiffusion; c'est ainsi que mon intérêt pour ce sujet s'est d'abord développé. J'ai ensuite travaillé pour IBM, aux États-Unis, et enseigné dans diverses universités américaines. De là, je suis venu à la faculté de droit Dalhousie, au Canada. Je travaille actuellement comme avocat à l'Institut de recherche et de réforme du droit, à l'Université de l'Alberta.

Le temps que j'ai été au Canada, j'ai préparé plusieurs rapports pour des ministères fédéraux, relativement à la politique de radiodiffusion, des télécommunications, et plus récemment, relativement à ce sujet.

Le Comité est sans doute curieux de savoir comment je suis finalement venu à m'intéresser à ce sujet. Le ministère de la Justice, en partie à cause de mes travaux antérieurs, m'a demandé un jour de l'aider à préparer un document de base sur les divers aspects de la criminalité informatique. Comme je suis fonctionnaire—d'une certaine façon, je suis chargé de conseiller le gouvernement de l'Alberta sur toutes ces questions—j'ai dû demander à mon institut de m'accorder du temps libre, ce qu'il a convenu de faire, en partie parce que la province s'intéresse à ce sujet également et en partie parce que les compétences en la matière se chevauchent.

Vous serez sans doute intéressés de savoir, en guise d'introduction, que la criminalité informatique n'intéresse pas seulement les sociétés de haute technologie du centre du Canada. Il y a déjà eu des problèmes dans les champs pétroliers. Les données sismiques informatisées ont déjà donné lieu à des poursuites.

Le ministère m'a permis de retourner aux États-Unis afin d'y visiter les études d'avocats qui se spécialisent dans ce domaine, de même que le professeur Richard Dole, qui a préparé une partie de la législation américaine dans ce domaine. Le ministère m'a également permis d'assister à la conférence de l'Association canadienne de l'informatique, et ainsi, d'avoir des contacts avec l'industrie.

[Texte]

I have submitted to the Department of Justice, and it is presently in draft form, a report, which includes some draft legislation. I undertook the work, of course, under an agreed arrangement between the institute and the Department of Justice. I do not think it is a matter for me to release that report, I think it is a matter for the Department of Justice. I do not think there should be too much difficulty about that.

• 1545

I trust you will appreciate my situation as a person who prepared a report, in effect, for two employers. I would suggest that what should be done is a communication in due course with Mr. Hill, at the Department of Justice, who is the project chief.

I also wanted—and there was a second reason, apart from the pure formalities of this matter... to check one or two details with various departments and people while I was in Ottawa, and make one or two editorial changes as soon as I get back to Edmonton. I have the draft here, and it will be available and finished by next week. So there is no time delay there.

As far as my status before the committee is concerned, I am appearing in my personal capacity. I have no brief of instructions from the Institute of Law Research and Reform or the Alberta government or the Department of Justice. At all times I have worked quite independently, and as I say, I have no formal brief or any particular position from anybody.

I thought what I could perhaps usefully do today, enabling the committee to pick up on any matters that it wished to address, is to outline to you my general position, and the details, as I say, appear in the documentation itself. In many ways, what I really wanted to try to do to assist you was to try to talk in a sense as a practical lawyer rather than in abstract, theoretical terms, because if my experience of parliamentary committees and congressional committees in the past is of any use to me, it is that a point is reached in these matters where one has to start saying, well, what are we going to do, and a sort of bottom line is reached.

I came into the matter virtually through two windows. It seemed to me that to grapple with the problem of computer crime one had to understand as best one could a fairly broad societal phenomenon, namely the sort of so-called information, post-industrial society that we live in, and then one had to break that down into various elements and try to understand certain components of that problem and the possible practical legal responses that can be made to it. I do not really want to say that much about the first one today, other than just to remind you of some salient features and then to deal more directly with what I see to be the legal problems.

It has been very common, of course, for the last decade now to talk of the arrival of a post-industrial society and of the importance of information generally. I am sure you have heard a great deal about these kinds of matters from the witnesses you have had before you. I have included in my report a summation of the sort of views that have been expressed by economists, communications theorists, global scientists, and

[Traduction]

J'ai soumis au ministère de la Justice un rapport préliminaire qui inclut un début de législation. J'ai évidemment entrepris ce travail dans le cadre d'une entente entre mon institut et le ministère de la Justice. Je ne suis évidemment pas en mesure de publier ce rapport. C'est au ministère de la Justice de le faire s'il le désire, mais je ne pense pas qu'il y ait de difficultés.

J'espère que vous comprendrez que je me trouve dans une situation délicate, étant donné que j'ai préparé un rapport pour deux employeurs. Il faudrait peut-être communiquer, en temps opportun, avec le chef du projet, M. Hill, du ministère de la Justice.

J'ai voulu aussi—et c'était là une seconde raison, à part les simples formalités de cette question—vérifier un ou deux détails avec les divers ministères, ainsi qu'avec certaines personnes, pendant que j'étais à Ottawa, pour apporter aussi une ou deux modifications au texte dès mon retour à Edmonton. J'ai le brouillon ici, et il sera disponible et terminé d'ici à la semaine prochaine. Il n'y a donc pas de retard à ce sujet.

Je comparais devant le Comité à titre personnel. Ni l'*Institute of Law Research and Reform* ni le gouvernement de l'Alberta, pas plus que le ministère de la Justice, ne m'ont donné d'instructions. J'ai toujours travaillé de façon autonome, et encore une fois, personne ne m'a confié de mémoire ni dicté une position, quelle qu'elle soit.

Pour permettre au Comité de choisir des questions qui l'intéressent, je pourrais peut-être aujourd'hui vous définir ma position générale, et les détails à cet égard figurent dans la documentation. Je vais essayer de vous parler en termes juridiques clairs, plutôt qu'abstraits et théoriques, parce que, d'après mon expérience des comités parlementaires et des commissions du Congrès, les choses progressent lorsque l'on commence à se demander ce qu'il faut faire, et que l'on commence à entrevoir des solutions.

Je me suis intéressé à cette question pour deux raisons. Il m'a semblé que pour saisir le problème des infractions relatives aux ordinateurs, il faudrait comprendre le mieux possible un phénomène social très large, je veux parler de la société post-industrielle, dite d'information, dans laquelle nous vivons; il faut ensuite examiner les divers éléments de ce phénomène, pour essayer de comprendre certaines des composantes de ce problème, et les solutions juridiques possibles pour y faire face. Je ne vais pas vraiment parler de ce premier aspect aujourd'hui, mais je voudrais simplement vous rappeler certaines caractéristiques, pour traiter ensuite plus directement de ce que je considère comme des problèmes juridiques.

Depuis 10 ans, on parle très couramment de l'émergence d'une société post-industrielle, et de l'importance de l'information, de façon générale. Je suis sûr que les témoins qui ont comparu devant vous vous ont beaucoup parlé de ces questions. J'ai inclus dans mon rapport un résumé des différents points de vue exprimés sur cette question par des économistes, des théoriciens des communications, des scientifiques et des

[Text]

sociologists on that sort of issue. I think we can probably say that as a result of all those studies over perhaps the last decade, we may have come to understand three things which I think are important to policy makers and to law draftsmen.

First of all, I think all those disciplines agree that somehow information involves a cybernetic type of process, and from that you have a very interdependent and linked kind of a society in which the free flow of information is critically important. The practical implication of that, of course, is that in any legal steps that you might choose to implement you have to be very conscious of not cutting down on that free flow.

Secondly, we have also come to understand how critical information in general is to our economic system, and where we stand, if you like, in the world pecking order. I probably do not need to do any more than remind you of the debate which has been emerging in recent weeks over the effectiveness of it in employment issues of that kind. You are well aware of that.

Thirdly, I think at another level it is clear from all these disciplines that certain kinds of human values are involved. Through the so-called "basic needs model" we understand that information is something that is very fundamental now to the human personality.

All of this tends to suggest that we are moving somehow to a society in which capital and labour theories of value are no longer as important as they were, and that we somehow live in a low-energy, high-information determined society. For instance, I can generate more information from even a hand-held calculator than from speaking the equivalent amount of energy here.

• 1550

All of these things were predictable; we were told they were going to happen by leading theorists over the last 10 years. I think we all understand that probably over the next quarter of a century they are going to mean changes in government, social arrangements and employability... probably in the nature of thought itself—and, of course, in legal ordering, which is particularly what this committee is concerned with. Reducing all of this back into a legal setting, the big problem for lawyers now, and probably for the next 20 or 30 years, is one I would call information entitlement: who gets information and under what circumstances? In general terms we accept that information is a good thing. I have not heard suggestions and my research has not uncovered anything which indicates that Canadian society somehow wants to predetermine what information we get. We accept it as a good thing and that we have as much of it as possible, except in some very limited areas, perhaps, involving national security. We also want to see it distributed through Canadian society so that we want to strike this balance between sufficient good information and its distribution to those who need and depend upon it. It seems very clear to me that government will have to resolve what I would call a whole series of entitlement issues over the years to

[Translation]

sociologues. Nous pouvons sans doute dire qu'à la suite de toutes ces études entreprises depuis 10 ans, nous pouvons peut-être comprendre trois points qui me paraissent importants pour les technocrates, ainsi que pour ceux qui rédigent les lois.

Tout d'abord, je pense que dans toutes ces disciplines, on convient que d'une façon ou d'une autre, l'information implique un processus cybernétique, de sorte que la société est très interdépendante, et le libre mouvement de l'information revêt une importance capitale. Naturellement, la conséquence pratique de tout cela, c'est que, quelles que soient les mesures juridiques que l'on voudrait appliquer, il faudrait s'assurer de ne pas freiner ce libre mouvement de l'information.

En second lieu, nous devons aussi en arriver à comprendre l'importance capitale de l'information, en général, pour notre système économique, et par rapport à notre rang parmi les autres nations. Il me suffit de vous rappeler le débat de ces dernières semaines au sujet de l'efficacité de cette question en ce qui concerne la situation de l'emploi. Et vous savez bien ce qu'il en est.

En troisième lieu, je pense qu'à un autre niveau, toutes ces disciplines montrent bien que certaines valeurs humaines interviennent aussi. D'après le modèle des «besoins fondamentaux», nous comprenons que l'information est quelque chose qui est maintenant très fondamental à la personnalité humaine.

Tout cela montre donc que nous nous orientons vers une société dans laquelle les théories valorisant le capital et le travail ne sont plus aussi importantes qu'auparavant, et que, d'une certaine façon, nous vivons dans une société où l'information très poussée repose sur peu d'énergie. Par exemple, je pourrais obtenir plus d'information d'une calculatrice, même de poche, qu'en vous parlant ici avec une dépense d'énergie équivalente.

Toutes ces choses étaient prévisibles, et les plus grands théoriciens nous les annoncent depuis 10 ans. Nous comprenons tous qu'au cours du prochain quart de siècle, cela devra entraîner des changements dans le gouvernement, les arrangements sociaux et l'emploi—il faudra probablement modifier notre façon de penser—et, bien sûr, les impératifs juridiques, questions qui préoccupent particulièrement ce Comité. Réduire tout cela à un cadre juridique, et c'est le grand problème qui se pose actuellement, et probablement au cours des 20 ou 30 prochaines années pour les avocats, nous amène à poser cette question: qui obtient l'information et dans quelles circonstances? De façon générale, nous admettons que l'information est une bonne chose. D'après mes recherches, rien n'indique que la société canadienne souhaite une prédétermination de l'information qu'elle obtient. Nous l'acceptons comme une bonne chose, et nous en voulons autant que possible, sauf peut-être dans des domaines très limités, impliquant la sécurité nationale. Nous souhaitons aussi qu'elle soit distribuée dans la société canadienne selon un critère double, de qualité et de distribution à ceux qui en ont besoin et qui en dépendent. Il me paraît très clair que le gouvernement devra résoudre, dans les années à venir, toute une série de questions de droit à l'infor-

[Texte]

come. I break those entitlement issues down into three categories, in my own mind at least—three big sub-questions. First of all: protection of information that is of commercial value; second, protection of private information that can spill into privacy-type issues; and third, the problem of government resource and information. Clearly, there is some inter-relationship between those three categories, although I think for analytical purposes and for practical purposes we need to deal with each of them.

I want to come now, against that very general background, which I have dealt with in much greater detail in the report, to the computer information sector specifically. I find the talk of computer crime or abuse is simply too broad; it is not a useful approach to the problem. It may be my particular mindset; I was trained as a traditional common lawyer. I believe that ultimately you have to identify fairly specific problems and deal with those. Although I appreciate the charge of many other disciplines that this amounts to a kind of intellectual reductionism and that you can lose sight of some of the bigger issues, ultimately you do have to face up to it in the day-to-day practice of law and I think also in the legislative process.

There are really two quite distinct things involved in computer crime, or so-called computer crime. First of all, there is what I would call unauthorized interference and second, so-called computer crime forms part of a much wider framework of improper trafficking in valuable information in general. My general perspective is that the first issue is much easier to resolve than the second one. It may assist you at this stage if I outline my general thesis and then come back and pick up perhaps on particular aspects of it.

My overall view of the state of Canadian law in general, both federal and provincial, is that it is deficient in both its criminal and civil law respects to deal with both of the specific issues I have mentioned. Second, I think that various kinds of law reform and some new laws at both the provincial and the federal level, and in both civil and criminal areas, is required. Third, being completely practical about it, I see no way that all of these problems can be solved all at once. I remind myself that institutions such as Harvard and Stanford have been working for 10 or 15 years in their law and technology programs with some very highly paid and high powered talent, and have made only a slight inroad into some of these particular problems.

As a professional law reformer, I am also prepared to accept the realities of the process and to try to establish some sort of priority as to what I think should be dealt with. I have no difficulty in settling for a third of a loaf or half of a loaf now, and a little more down the line. I have spent sufficient time around legislatures in several parts of the world to think that one has to be that realistic in what one can expect to get done.

[Traduction]

mation. À cet égard, je voudrais distinguer trois catégories et trois grandes sous-questions. Tout d'abord, la protection de l'information qui revêt une valeur commerciale; deuxièmement, la protection des renseignements personnels qui peuvent aboutir aux questions de droit à la vie privée; et troisièmement, le problème des ressources et de l'information du gouvernement. Il existe manifestement des relations entre ces trois catégories, mais aux fins de l'analyse, et pour des raisons pratiques, il nous faut les examiner chacune séparément.

Dans le cadre de ce contexte très général, que j'ai examiné de façon beaucoup plus détaillée dans le rapport, je voudrais en arriver maintenant, de façon plus précise, au secteur de l'information automatisée. Parler d'infractions ou d'abus relatifs aux ordinateurs me paraît trop général; ce n'est pas une façon utile d'aborder le problème. C'est peut-être là une déformation personnelle ou professionnelle, car ma formation est celle d'un avocat traditionnel spécialisé dans le droit commun. Je crois qu'en dernière analyse, il faut définir des problèmes très précis à examiner. Selon les porte-parole de beaucoup d'autres disciplines, cela revient à une sorte de «réductionnisme» intellectuel qui risque de faire perdre de vue certaines questions plus vastes, mais en dernière analyse, il faut affronter ces difficultés dans la pratique quotidienne du droit, et aussi, je crois, dans le processus législatif.

En fait, deux éléments très distincts interviennent dans ce que l'on qualifie d'infractions relatives aux ordinateurs. Tout d'abord, il y a ce que je qualifierais d'interférence illégale, et en second lieu, ces dites infractions constituent un élément d'un ensemble plus vaste, celui du trafic illégal d'informations valables en général. D'après ma perspective générale, la première question est beaucoup plus facile à résoudre que la seconde. Il serait peut-être utile à vos travaux que je vous définisse maintenant ma thèse générale, pour revenir ensuite à certains de ces aspects.

Dans l'ensemble, je trouve que le droit canadien, aussi bien fédéral que provincial, présente des lacunes par rapport aux deux questions précises que j'ai mentionnées, et ce, aussi bien en ce qui concerne le droit criminel que le droit civil. Par ailleurs, je pense que diverses réformes du droit s'imposent, de même que certaines nouvelles lois, au niveau provincial aussi bien que fédéral, en ce qui concerne les domaines civils et criminels. Troisièmement, étant tout à fait pratique à ce sujet, je ne vois nullement que tous ces problèmes puissent être résolus à la fois. Je me dis que des institutions comme Harvard et Stanford travaillent depuis 10 ou 15 ans dans le domaine juridique et technologique, avec un personnel très bien payé et extrêmement compétent, et malgré tout cela, les progrès n'ont été que modestes.

En tant que spécialiste de la réforme du droit, je suis aussi disposé à accepter les réalités du processus et à essayer d'établir certaines priorités quant aux questions à examiner. Je n'ai pas de difficulté à limiter les ambitions au départ, car je sais que les résultats n'en seront que meilleurs. J'ai passé suffisamment de temps dans des assemblées législatives, dans

[Text]

✓

What I personally would like to see is what I would call a staged, pragmatic approach along the following lines. First of all, at the level of Criminal Code reform I think there is a strong case for a certain kind of reform directed to preserving what I am going to call, just for a phrase at this stage, the integrity of the computer system and data retrieval systems. I will come back and explain what I mean by that.

Basically, that is a prophylactic device. Both on my own research and discussions with industry, I think it would go some distance toward meeting the kinds of concerns which brought about this sort of inquiry in the first place. Secondly, in general I think the second issue of improper trafficking in commercially valuable information would be better left in the first instance to civil law reform.

There are four categories where civil law reform is appropriate. First of all I strongly support and hope would proceed apace the present review of the federal Patent Act and Copyright Act, and the fact that I am not going to say much about that in this presentation should not be taken as detracting from the fact that I support that effort. That is at the federal level. Secondly, I do believe that at the provincial level there is a strong case for a review of trade secret law with a view to possible implementation of uniform trade secret protection laws. Thirdly, the time is ripe, I think, for a review of so-called restrictive covenants in contracts. Fourthly, the time is also ripe for a review at the provincial level of the whole notion of unfair competition. In terms of priorities as between those four, I personally think copyright review and trade secret law review probably should receive priority if it comes to a question of allocation of resources.

The third step in my equation, if one is trying to arrive at some sort of comprehensive national blueprint, is that once you know the shape of what is being done in my second category—that is, copyright law or trade secret law, contract and so forth—you might possibly wish to consider the criminalization of theft of trade secrets, not necessarily because of its domestic application but because of its possible use in external situations, by which I mean the sort of situation we had where Japan recently appropriated some U.S. trade secrets. The difficulty with considering criminal trade secret laws at the present time, of course, is that the concept is still somewhat undefined in Canadian domestic law. Also, there is an argument—and I think quite a forceful argument—that can be made that it would be inappropriate to consider criminal law proscription of something which is not civilly redressable.

The fourth step in my equation is that I would not presently recommend any Criminal Code offence—or other regulatory offence, for that matter... at the federal level being imposed upon the data processing industry itself for failure to take adequate and reasonable care. In my view, this certainly is a serious issue that will need to be addressed in due course, relating to the security of computer-type information as it affects the parties. I am sure you have probably heard already from witnesses who would express this kind of concern.

[Translation]

plusieurs pays du monde, pour savoir qu'il faut avoir des ambitions réalistes.

Personnellement, je voudrais une façon progressive, pragmatique d'aborder les choses, selon les perspectives suivantes. Tout d'abord, en ce qui concerne la réforme du Code criminel, je crois qu'elle devrait préserver ce que je qualifierai, pour le moment, d'intégrité des systèmes d'ordinateurs et des systèmes de recherche des données. Je reviendrai là-dessus pour expliquer ce que j'entends par là.

Fondamentalement, il s'agit là d'un moyen prophylactique. D'après ma propre recherche et des discussions avec l'industrie, il aura une certaine utilité pour répondre aux préoccupations qui ont été à l'origine de cette enquête. Deuxièmement, de façon générale, je pense que la deuxième question, celle du trafic illégal d'informations ayant une valeur commerciale, devrait plutôt relever de la réforme du droit civil.

Cette réforme conviendrait pour quatre catégories. Tout d'abord, j'appuie fortement la révision actuelle des droits fédéraux sur les brevets et sur le droit d'auteur, et j'espère qu'elle ira bon train; je ne vais pas en parler longuement au cours de cet exposé, mais il ne faut pas y voir une critique de cet effort que j'appuie pleinement. Voilà pour le niveau fédéral. Par ailleurs, je crois qu'au niveau provincial, il faudrait vraiment revoir les lois sur les secrets de fabrication, afin qu'elles puissent s'appliquer de façon uniforme. Troisièmement, il est temps, je crois, de revoir les soi-disant stipulations restrictives des contrats. Quatrièmement, il est temps aussi de revoir, au niveau provincial, toute la notion de la concurrence déloyale. Si l'on voulait fixer une priorité par rapport à ces quatre catégories, je l'accorderais personnellement à la révision des lois sur le droit d'auteur et sur les secrets de fabrication, et la question qui se pose est celle de l'attribution des ressources.

Le troisième élément de mon équation, si l'on essaye d'en arriver à une sorte de grille nationale, c'est qu'une fois que l'on sait ce qui se fait dans ma seconde catégorie—c'est-à-dire les lois sur le droit d'auteur ou sur les secrets de fabrication, les contrats, et ainsi de suite—l'on pourrait souhaiter envisager de criminaliser le vol de secrets commerciaux, pas nécessairement en raison de leur application nationale, mais plutôt de leur utilisation possible à l'étranger, et je veux parler à cet égard de ce qui s'est passé récemment au Japon, lorsque ce pays s'est approprié certains secrets commerciaux des États-Unis. La difficulté d'une telle entreprise, c'est qu'actuellement, le concept est encore assez mal défini dans le droit national canadien. De plus, certains estiment—et avec de bons arguments—qu'il ne conviendrait pas de faire tomber sous le droit criminel des délits réparables en droit civil.

Le quatrième élément de mon équation est que je ne suis pas prêt à recommander qu'au niveau fédéral, on reconnaisse l'industrie du traitement des données coupable d'infractions criminelles—ou de toute autre infraction prévue dans les textes réglementaires, d'ailleurs—pour n'avoir pas pris des précautions suffisantes et raisonnables. C'est, selon moi, une question très importante, dont il faudra s'occuper en temps opportun; elle concerne la sécurité des renseignements informatisés par

[Texte]

• 1600

I remind you that it is relatively elementary public policy analysis that there are a number of alternatives that could engage that area. First of all, of course, there was the possibility of self-regulation by the industry. One would need to know just how effective industry regulation is.

Secondly, if one thought it were not effective, one might have to consider various kinds of regulatory schemes falling short of a Criminal Code offence, and I have mentioned some of those in my report. I would regard it as a third and last alternative, particularly bearing in mind the kind of criteria which have been involved for federal criminal law reform in this country, to consider putting an offence of that kind into the present omnibus bill.

You will appreciate then that my scheme of things, if I can put it that way, involves doing certain kinds of things in the present omnibus bill, certain kinds of things which necessarily would have to be done, I think, on a collaborative basis between the federal government and the provinces and might involve the evolution of a suitable mechanism to get uniform legislation.

Thirdly, once you know what the dimensions of those reforms would be, they might then... coming back to consider, if you like, the residue that might need to be picked up in the future from the law review.

Against that background, I wanted to turn back now and discuss the interference problem with computers, if I might, in a little more detail.

I always used to tell my students—I grew up on a farm, and for some reason I like homely analogies; it seems to open the matter up. I have always conceptualized this problem of information as involving, if you like, a chicken coop in the middle of a yard with a chicken in it. The chicken represents the piece of information, and the coop represents whatever it is that the information is in. It may be a computer or it may be something else. Two kinds of things can happen. Somebody can open the door and let the chicken out, and various things can then happen to the chicken. The question is: What are you going to do? Are you going to try to stop people from opening the door, or are you going to worry about what happens to the chicken when, if you like, it goes farther down the yard and disappears?

The next question I then ask myself is: Why do people open the door?—without getting into a whole lot of computer jargonese, which just tends to confuse matters. Basically, they do it for one of two reasons. Either they are the Moriarty type in society, which in New Zealand we call the Everest syndrome: it is there, you want to try it; you are a student, you just cannot bear not to try it. There is a slight degree of quirkiness, of inquiry, that may not even necessarily be a bad thing in society. You want to see what happens when you open the door.

[Traduction]

rapport aux parties intéressées. Je suis sûr que des témoins vous ont déjà parlé de ce genre de préoccupations.

Je voudrais vous rappeler que selon une analyse élémentaire de la politique publique, il existe un certain nombre de possibilités à propos de cette question. Tout d'abord, celle d'une autoréglementation par l'industrie. Il faudrait simplement savoir si la réglementation de ce secteur est efficace.

En second lieu, si elle ne l'était pas, on pourrait envisager divers moyens de réglementation, à l'exclusion d'une infraction criminelle, et j'en ai indiqué certains dans mon rapport. En troisième et dernière possibilité, il faudra tenir compte en particulier des critères mis au point dans ce pays pour la réforme du droit criminel fédérale, où il était question de considérer qu'une infraction de ce genre s'intègre dans le bill omnibus actuel.

Mon système, si je peux le qualifier ainsi, implique donc que l'on fasse certaines choses dans le bill omnibus actuel, choses qu'il faudrait sans doute faire en collaboration entre le gouvernement fédéral et les provinces, et qui pourrait impliquer l'évolution d'un mécanisme convenable, pour que les lois s'appliquent de façon uniforme.

En troisième lieu, une fois que vous savez quelles seraient les dimensions de ces réformes, il pourrait alors y avoir... L'on pourrait peut-être envisager ce qu'il resterait à faire à l'avenir, à partir de la révision du droit.

Dans ce contexte, je voudrais maintenant revenir en arrière et discuter des problèmes d'interférence avec les ordinateurs, et ce, de façon un peu plus détaillée.

Je disais toujours à mes étudiants... j'ai grandi dans une ferme, et pour cette raison j'aime les exemples familiers, qui semblent bien expliquer les choses. J'ai toujours conceptualisé ce problème de l'information en l'illustrant ainsi: une cage au milieu d'un champ, avec un poulet dedans. Le poulet représente l'élément d'information, et la cage, le contenant de cette dernière. Ce peut-être un ordinateur, par exemple. Il peut se passer deux choses. Quelqu'un peut ouvrir la porte et laisser sortir le poulet, et toutes sortes de choses peuvent lui arriver. Que faut-il faire? Faut-il essayer d'empêcher les gens d'ouvrir la porte, ou faut-il se préoccuper de ce qu'il adviendra au poulet s'il s'écarte du champ et qu'il disparaît?

La question que je me pose ensuite est celle-ci: pourquoi des gens ouvrent-ils la porte de la cage? Je n'ai pas besoin de faire intervenir énormément de jargon relatif aux ordinateurs, qui complique en général les choses. Essentiellement, les gens ouvrent cette cage pour une ou deux raisons. Ou bien ils vivent dans une société de type *Moriarty*, dont nous parlons, en Nouvelle-Zélande, comme du syndrome de l'Éverest: il est là, on essaie de s'y attaquer, un étudiant ne pourrait y résister. Il y a donc là une curiosité d'esprit qui n'est pas nécessairement mauvaise dans une société. Des gens voudraient savoir ce qui se passe une fois que la porte est ouverte.

[Text]

At the second level, of course, the second kind of person is the man or woman who opens the door for profit, the mammon element, if you like, in these kinds of things. You can partially address the second element by forcing the door to stay closed. I do think, and I urge it on you as an analogy, that what you are really after at the present time, and I think you would be performing an important and valuable service—the protection of the integrity of the coop, if I can stick with my analogy, can be protected through Criminal Code prescription. That probably would involve the creation of two kinds of offences. First of all, clearly, you should be concerned about the unauthorized use of the computer system; and secondly, you would want to try to prescribe or make it an offence to meddle with data within such a system in various ways. As I have suggested to you, that would be both prophylactic and would also address a particular kind of harm that can be defined and has been defined in other statutes. As to the chicken going down the road and all sorts of misadventures befalling him, you will appreciate that my argument is that I would like to know what is going to happen on the civil law side before I made some final decisions on what, if any, criminal proscription should be there.

• 1605

I have a number of reasons of a more theoretical character as well for that. My first argument, of course, is entirely a practical one as to what you can really expect to get done at this time. You will appreciate from my paper that I have a fundamental difficulty with treating information as property for the purposes of criminal law proscription, for reasons that I have outlined. Its economic characteristics are not such as lend it very readily to a property law concept, so that something like theft of information, putting that into the code, I think is largely ineffective and is not so much ineffective as outweighed by the very substantial disadvantages it would carry elsewhere in society. I am concerned about the effect it would have on employment mobility and questions of that kind; I have dealt with those in my paper.

I perhaps should add one other thing, which may be puzzling you and which has troubled a lot of theorists in the States, and that is the question: Am I troubled at all by a system of concurrent remedies? The answer is: Not at all. There was and has been an ongoing debate, I suppose for about 10 years, in the States between lawyers advising on the construction of laws in this area as to whether it matters if you have different laws, both at the federal and provincial levels, and several possible alternatives that are open to an affected person. I have never lost any sleep about that. It poses very few practical problems. The only things you have to be aware of in the drafting sphere are that sometimes you get the odd jurisdictional problem as between courts and sometimes you might get some limitations problems—that is, the time within which an action must be brought—and occasionally you get the potentiality of some remedial problems, particularly in the civil sphere, with the possibility of double recovery of damages and things like that. But none of those things, which lawyers

[Translation]

Au second niveau, bien sûr, la personne qui ouvre la porte le fait pour le profit, car il entre un élément de iucre dans ce genre de choses. On peut résoudre en partie cette difficulté en forçant, en quelque sorte, la porte à rester fermée. Je pense, et je vous prie de me suivre dans cet exemple, que ce que vous recherchez vraiment maintenant—et vous offrirez, je crois, un service important et utile—c'est la protection de l'intégrité de la cage—et je m'en tiens à mon exemple—grâce aux prescriptions du Code criminel. Le procédé impliquerait la création de deux types d'infractions. Tout d'abord, vous devriez vous préoccuper de l'utilisation illégale du système d'ordinateurs; et en second lieu, vous voudriez essayer d'établir certaines règles, ou de dire que c'est une infraction que de toucher aux données d'un tel système, selon certaines modalités. Comme je vous l'ai dit, ce serait un bon moyen prophylactique, de même que ce serait un moyen de régler un problème qui peut être défini et qui l'a été dans d'autres lois. Quant au poulet qui s'égare sur la route et à qui toutes sortes de mésaventures arrivent, vous comprenez sans doute que j'aimerais savoir ce qui se passera au chapitre du droit civil, et ce, avant de prendre une décision définitive quant aux interdictions pénales à imposer dans ce cas.

J'ai aussi un certain nombre de raisons de nature plus théorique. Mon premier argument, bien sûr, est entièrement ordre pratique, puisqu'il s'agit de déterminer ce qu'il est vraiment possible de faire pour le moment. D'après mon document, vous comprendrez sans doute que j'ai beaucoup de mal à considérer l'information comme un bien aux fins des proscriptions du droit criminel, pour les raisons que j'ai soulignées. Ces caractéristiques économiques sont telles qu'elles ne se prêtent pas très aisément au concept de la propriété défini en droit, de sorte que prévoir, dans le code, le vol de l'information sera essentiellement inefficace, mais il faut surtout penser au très grand désavantage d'une telle solution pour le reste de la société. Je me préoccupe, par exemple, de ses répercussions sur la mobilité de la main-d'oeuvre et des questions de ce genre; j'en ai traité d'ailleurs dans mon mémoire.

Je devrais peut-être ajouter autre chose, qui vous étonnera peut-être beaucoup et qui a gêné beaucoup de théoriciens aux États-Unis; il s'agit de cette question: est-ce que je tiens vraiment à ce qu'il y ait un système de réparation commun? Pas du tout. Depuis environ 10 ans, des juristes américains discutant de l'élaboration de lois dans ce domaine se demandent s'il y aurait des difficultés du fait de l'existence de lois différentes, au niveau fédéral et provincial, et des nombreuses solutions possibles dont pourrait se prévaloir une personne lésée. Je n'ai jamais passé de nuit blanche à ce sujet. Il y a là très peu de problèmes pratiques. Les seules choses dont il faut être conscient dans la rédaction des lois, c'est qu'il se pose exceptionnellement des problèmes de compétence entre tribunaux, et parfois, il peut y avoir certains problèmes de limitation—je veux parler des délais afférents aux actions à intenter—et parfois, il peut se présenter certains problèmes quant aux réparations, en particulier en droit civil, avec la possibilité de doubles dommages et intérêts, et ainsi de suite.

[Texte]

are quite used to coping with, I think, pose any insuperable difficulties to the general notion of concurrent remedies.

If it were possible to achieve the sort of staged approach that I am suggesting, I suspect that it would involve really reconciling oneself, as a legislator, to the notion that certain things can be done now. The second level of things that I have mentioned could be urged as being necessary, and you would then be faced with the mechanical problem of how to carry those kinds of reforms forward.

That is my position in very round and general terms, Madam Chairman. I wondered if it might be more appropriate—I did not want to speak on here in a unilateral way—if, having indicated my general position, and once Mr. Fisk has elaborated on his concern, I then dealt specifically with any matters you wished to raise.

Mr. George E. Fisk (Counsel, Gowling and Henderson Barristers, Ottawa, Ontario): Thank you. I am afraid I cannot say anything about chickens; I will leave that to Dr. Hammond as the expert on the subject.

As to my background on the matter, I am a member of a large law firm, we have offices in both Ottawa and Toronto. Within that firm I run a computer law group. At the moment, we have about six lawyers who work with that group, either part time or full time. They all have scientific degrees; three of them have master's degrees in the computer field in one way or other. I also teach industrial property. So I see it from two sides: I see it from the side of clients who are very concerned about protecting their software and I also see it from the side of students to whom I am teaching standard industrial property patents, trademarks, copyright principles.

• 1610

✓ I have said in my material that most of my clients strike me as being paranoid. That is not necessarily bad. It always helps to be paranoid when you have something to be paranoid about. And when you are trying to protect information, it really does help to be paranoid, because if you look at it, you are spending years, person-years, in developing this information. You have to come up with the money to employ programmers. The programmers sit there and write code; and writing programs is not an easy thing. People think it is a very good day when they have written 100 lines. That is amazing. A hundred lines in a day is good. A program of 15,000 to 20,000 lines takes a long time to prepare. You have it prepared, you are just about to go out onto the market and you are about to sell it or license it; along comes somebody who takes the disc or the tape on which that program is included and puts that disc or program in a simple copier, and within a minute they have another copy of that program. They can go out and sell theirs perhaps even before you go out.

One of the interesting things we have found with video games is that many of these games are developed in Japan, and before the legitimate games reach Canada—the ones that are

[Traduction]

Mais aucune de ces difficultés, que les avocats ont bien l'habitude de résoudre, ne pose de problème insurmontable quant à la notion générale de réparations communes.

S'il était possible d'appliquer la solution progressive que je recommande, il faudrait, je crois, se réconcilier, en tant que législateur, avec l'idée de concrétiser déjà certaines choses. J'ai mentionné un second niveau, et là, les choses me semblent vraiment nécessaires; on serait ensuite confronté aux problèmes techniques, à savoir comment appliquer ce genre de réforme.

Madame le président, voilà donc, en termes très généraux, quelle est ma position. M. Fisk va présenter son point de vue, et ensuite, il conviendrait peut-être davantage que je traite de façon précise de questions que vous voudriez soulever.

M. George E. Fisk (avocat, Gowling and Henderson Barristers, Ottawa, Ontario): Merci. Je crains de ne pouvoir parler de poulets. Je laisserai cela à M. Hammond, qui sera donc le spécialiste de la question.

Je me permettrai de vous rappeler que je suis membre d'une grande étude juridique, et que nous avons des bureaux à Ottawa, ainsi qu'à Toronto. Dans cette étude, je dirige un groupe qui étudie les questions juridiques en rapport avec les ordinateurs. Pour le moment, six avocats travaillent dans ce groupe, à temps partiel ou à plein temps. Ils ont tous des diplômes scientifiques; trois d'entre eux ont un diplôme de maîtrise dans le domaine des ordinateurs, sous toutes sortes d'angles. Je donne aussi un cours sur la propriété industrielle. Je considère cette question selon deux perspectives: du point de vue des clients qui tiennent à protéger leur logiciel, et du point de vue de mes étudiants, à qui j'enseigne les brevets uniformes de propriété industrielle, les marques de commerce, les principes du droit d'auteur.

J'ai dit dans mon mémoire que la plupart de mes clients me paraissent paranoïaques. Ce n'est pas nécessairement une mauvaise chose. Il est toujours utile de l'être quand on a quelque chose qui exige qu'on le soit. Et quand on essaie de protéger l'information, il est vraiment utile d'être paranoïaque, car, à bien considérer les choses, on dépense de l'argent, des années-personnes à élaborer cette information. Il faut trouver de l'argent pour employer des programmeurs. Ces derniers travaillent donc et écrivent en code; il n'est pas facile de rédiger un programme. Des programmeurs sont très satisfaits d'eux-mêmes parce qu'ils ont écrit 100 lignes en une journée. C'est incroyable. Il faut très longtemps pour préparer un programme de 15,000 à 20,000 lignes. Une fois qu'il est prêt, il faut aller le vendre, ou le faire breveter; or, quelqu'un vient, prend le disque ou le ruban sur lequel le programme a été enregistré, et il l'insère dans un simple duplicateur; au bout d'une minute, il obtient un autre exemplaire de ce programme. Il peut sortir et le vendre en un temps record.

L'une des choses intéressantes que nous avons découvertes à propos des jeux vidéo, c'est que beaucoup sont fabriqués au Japon, et beaucoup entrent au Canada du fait des activités de

[Text]

licensed by the owners of those games, the creators... infringers have stolen the games and have brought them to Canada even ahead of the people who developed them and are making money from them. So companies are very afraid that their information is going to be taken.

There are two ways to protect the information: you can do it by technological means and you can do it by legal means. Technological means are such tricks as encoding. You put the program in code, or restrict access, keeping your source code under lock and key, or using passwords or something of that sort.

I should, for those who do not know the difference between source and object code, say that a computer is operated by a program in object code, which is a series of ones and zeros. But if you want to do something to that program, if you want to correct it or if you want to understand how it works, so you can add to it, you really need the source code. In most cases that is in human-readable language. So some companies will let out the object code to people who need to have it, but the source code is kept in a vault. It is kept in a place where it cannot easily be reached.

In some extreme cases—and this occurs particularly where the company makes not only the software but also the computers on which it runs—the company may devise an entirely new computer language just for its software, just so that nobody else can understand the language. It makes it harder for people to copy it.

So there are technological means. However, what can be done with technology can usually be undone with technology as well. I could, for example, go out of this room today, walk up O'Connor Street about four blocks, and go into a small store there and buy a program called *Locksmith*. That program is on sale in Ottawa, perfectly legally, and what that program is to do is to take out the coding on coded programs. It is quite effective. People do their best to code a program, along comes a program like *Locksmith*—and there are a number of others around—and you can take it and destroy that coding and then use this coded program in any way you want. That is perfectly legally available in Canada, as are a number of others. They are also widely advertised in computer magazines and very easily available.

• 1615

There are also clubs—one of them exists in Ottawa, for example—whose main function is for people to come together, take the programs they have decoded, and exchange copies. Everybody gets copies of everybody else's programs. That, of course, destroys the market for the company that sells these programs; that company sells one copy, but there may be 200 in the club. They just lost 199 other possible sales. This goes on at the moment. So you can see why companies are paranoid. There are technological ways to make it difficult to copy programs, but they are not completely effective. They do maybe discourage the very novice person.

[Translation]

certaines «pirates», qui travaillent plus vite que les propriétaires, les créateurs qui ont fait breveter ces jeux. Les compagnies ont donc très peur que leur information ne soit volée.

Il existe deux sortes de moyens, technologiques ou juridiques, de protéger l'information. Les premiers impliquent un codage. Le programme est enregistré en code, à moins qu'on en limite l'accès, et que le code d'origine reste sous clé, ou que l'on utilise des mots de passe, par exemple.

Pour ceux qui ne connaissent pas la différence entre le code de source et le code objet, disons qu'un ordinateur fonctionne selon un programme, en code objet, qui est une série de uns et de zéros. Si vous voulez faire quelque chose de ce programme, si vous voulez le corriger ou comprendre comment il fonctionne, afin de pouvoir l'augmenter, vous avez en fait besoin du code d'origine. Dans la plupart des cas, il s'agit d'un langage lisible. Par conséquent, certaines sociétés font connaître le code objet aux personnes qui en ont besoin, mais elles gardent le code d'origine dans un coffre auquel il est difficile d'avoir accès.

Dans certains cas extrêmes, et cela se présente surtout lorsque des sociétés fabriquent non seulement le logiciel, mais aussi les ordinateurs, on peut mettre au point un langage machine entièrement nouveau, rien que pour le logiciel, afin que personne d'autre ne puisse le comprendre. La reproduction devient donc plus difficile.

Il existe donc des moyens technologiques. Cependant, la technologie peut défaire ce qu'elle a fait. Par exemple, je pourrais quitter cette pièce aujourd'hui, remonter la rue O'Connor sur quatre coins de rue et entrer dans un petit magasin pour acheter un programme intitulé *Locksmith*. Ce programme se vend à Ottawa, de façon tout à fait légale, et il permet de décoder des programmes codés. Il est très efficace. Des gens s'efforcent de coder un programme, puis survient un autre, comme *Locksmith*, et beaucoup d'autres encore, qui peut détruire ce codage et être utilisé de toutes les façons possibles. C'est là quelque chose de tout à fait légal au Canada, comme beaucoup d'autres programmes d'ailleurs. Ils font l'objet d'une très grande publicité dans les magasins spécialisés dans les ordinateurs, et il est très facile de se les procurer.

Il existe aussi des clubs—il y en a par exemple un à Ottawa—dont la principale fonction est de réunir des gens qui échangent des copies des programmes qu'ils ont décodés. Tout le monde obtient des copies des programmes de tout le monde. Cela détruit bien sûr le marché de la compagnie qui vend ces programmes. Elle en vend un, mais il peut en exister 200 dans le club. Elle a simplement perdu 199 autres ventes possibles. Voilà ce qui se passe maintenant. Vous comprenez pourquoi les compagnies sont paranoïaques. Il existe des moyens technologiques de rendre difficile la copie des programmes, mais ils ne sont pas efficaces. Ils ne découragent peut-être que les novices.

[Texte]

I was amused awhile back. I was watching *Computer Academy* on TV Ontario, which has been running for the past month or two, and one very naive question was asked by somebody at the end, saying: I bought a computer game and put it into my computer, then I typed in "list", and it would not list its program. Why not? Of course, the reason was that the program was encoded. You have to do a little bit more than just putting in the word "list" to find out what that program is. But many users tend to expect they have an absolute right to copy any program they have acquired by fair means or foul, and to pass it on to anybody else who wants it.

That, of course, if it became widespread, would destroy the entire market for programs, and would destroy the incentive for people to spend those years in writing the programs, because you are not going to spend the money to hire programmers unless you get something back.

However, at the moment, people are using technological means to try to protect against unauthorized copying. Just to give you an idea of how widespread copying is, I gave you in my material a reference to a case that was recently heard in Toronto dealing with the video game *Donkey Kong*. That is a video game which is very popular these days, and the president of the company who can legally sell that game in Canada testified that out of every ten *Donkey Kong* games in the Toronto area, nine of them were forgeries. In other words, that is the scale of the problem.

So people try with technological means; they are not very effective. I have two complaints about technological means. First, they do not work very well. They are almost a game. The type of programmer that Dr. Hammond referred to was Moriarty programmers; they take technological protection as a skill-testing question. They want to see whether they can break it. The more complicated the technological protection, the more fun they have.

To give you an example of that, I also noticed that when pay-television came to the City of Edmonton there was a contest at the Northern Alberta Institute of Technology, between the students, to see who could break the pay television code first and get it for free. It took the winner two days. Furthermore, the winner was such a hero he was interviewed on *As It Happens*. This gives a terrible impression to other people in the country. Not only is it all right to copy somebody's games or to break into their pay television, but you are a hero if you do. You get on national radio. So the wrong mind-set is being created.

Mr. Beatty: Maybe we need amendments to the CBC Act.

Mr. Fisk: Something along that line, perhaps.

So the first problem I have with technological protection is it does not work very well. Second, it seems to me to be awfully wasteful to have good programmers busting their brains to try to find ways of protecting programs, and equally good programmers busting their brains to find ways of overcoming

[Traduction]

Ce que j'ai vu il y a quelque temps m'a amusé. Il s'agissait du programme «*Computer Academy*», sur TV Ontario, qui est présenté depuis un mois ou deux, où quelqu'un avait posé une question très naïve à la fin du programme; il avait acheté un jeu informatique qu'il avait inséré dans son ordinateur, et lorsqu'il avait appuyé sur le bouton «enregistrer», son programme n'était pas enregistré. Il se demandait pourquoi. C'est qu'évidemment, le programme était codé. Il faut faire un peu plus que d'appuyer sur le bouton «enregistrer», pour savoir ce qu'est ce programme. Mais beaucoup d'utilisateurs ont tendance à croire qu'ils ont le droit absolu de copier n'importe quel programme qu'ils ont acquis par des moyens légaux ou non, et de le transmettre à tous ceux qui voudraient l'avoir.

Évidemment, une fois répandu, cet usage détruirait tout le marché des programmes, et plus personne ne voudrait passer toutes ces années à écrire des programmes, parce que personne ne voudra dépenser de l'argent pour engager des programmeurs, à moins de faire un profit.

Cependant, maintenant, on utilise des moyens technologiques pour essayer de se protéger contre la duplication illégale. Pour vous donner une idée de l'étendue de cette duplication, je vous ai indiqué dans mes documents une référence à une affaire dont il a été récemment question à Toronto, traitant du jeu informatique *Donkey Kong*. C'est un jeu vidéo très populaire ces temps-ci, et le président de la société qui peut légalement le vendre au Canada a témoigné que sur 10 jeux *Donkey Kong* en vente dans la région de Toronto, neuf étaient des faux. Voilà qui situe bien l'ampleur du problème.

Par conséquent, encore une fois, on essaie les moyens technologiques, mais ils ne sont pas très efficaces. J'aurais deux critiques à faire à ce sujet. Tout d'abord, ces moyens ne fonctionnent pas très bien. C'est presque un jeu. M. Hammond a parlé des programmeurs «Moriarty», pour eux, la protection technologique est une sorte de défi à leur compétence. Pour eux, c'est une gageure, et plus la protection technologique est complexe, plus ils s'y intéressent.

Pour vous en donner un exemple, j'ai aussi constaté que lorsque la télévision payante est arrivée à Edmonton, il y avait une compétition, au *Northern Alberta Institute of Technology*, entre les étudiants, pour voir qui pourrait décoder le premier la télévision payante et l'obtenir gratuitement. Le gagnant s'y est consacré pendant deux jours. En outre, c'était un tel héros qu'il a été interviewé à l'émission *As It Happens*. L'impression que cela donne aux autres Canadiens est incroyable; non seulement il n'y a aucun mal à copier les jeux d'une société ou à décoder la télévision payante, mais on devient un héros si on y réussit. On accède par là à la radio nationale. Voilà comment se crée un état d'esprit inadmissible.

M. Beatty: Il faudrait peut-être modifier la Loi sur la société Radio-Canada.

M. Fisk: Peut-être, en effet, . . .

Le premier problème quant à la protection technologique, c'est donc qu'elle ne fonctionne pas très bien. En second lieu, il me semble que c'est un gaspillage incroyable que de demander à de bons programmeurs de s'escrimer à trouver des moyens de protéger des programmes, alors que des programmeurs aussi

[Text]

those protections. These are non-useful ways of spending time. They do not add to the total amount of useful programming in the country and yet a lot of very intelligent people are spending their time on it. So it seems to me that it is really a futile or frustrating exercise.

• 1620

The other thing of course that concerns me about technological means of protection is that the mere fact that companies think they are necessary is, in my mind, quite an indictment of our legal system. If the legal system was doing its job, things like that would not be necessary. Programmers would not need to spend their time protecting programs in this way.

Now we come to the legal means of protection. They divide naturally into criminal law and civil law, and the civil law means are basically trade secrets, patents and copyright. Criminal law, to the people that I deal with, the companies in the field, generally is not a preferred way of protecting computer software.

The reason for this is that the basic approach in criminal law is to punish. The company that has had its software stolen, does not really care very much about punishment; what it wants is recompense. Therefore criminal law does not really address the problem the company has. From a commercial firm's point of view, criminal law is a very ineffective way of going about this.

For one thing, once you have turned over the matter to the police or to the Crown attorney, you have no more control over it. If I, to use the colloquial term, lay a charge, if I go down to the police station and ask them to lay charges, or I go down to the Crown attorney, then the Crown is prosecuting. I have no other status in the matter. I may be called as a witness but I cannot say: Look, I have changed my mind, I do not want to prosecute this guy any more. Therefore, if the person comes to me and says he is sorry and will pay for the program, I cannot withdraw the charge; only the Crown can do that. There is no flexibility; there is no possibility of a settlement.

So the company does not like to lay criminal charges, because there is no real advantage to it from this. I might add that there is also a terrible disadvantage to the public at large, because criminal prosecutions can be very expensive. I have one where we did lay charges and one poor RCMP officer has been working on that for six months solid—I believe full time, although I am not sure of that. There is this problem then with criminal charges, that there is no flexibility and that the aggrieved person cannot withdraw the charges.

[Translation]

compétents s'escriment, de leur côté, à trouver des moyens de déjouer ces protections. C'est là du temps gaspillé inutilement. Cela n'ajoute rien au total des activités de programmation utile qui se déroulent au Canada, et pourtant, il y a énormément de gens très intelligents qui y passent tout leur temps. Cela me semble dès lors une activité aussi inutile que peu enrichissante.

Un autre élément qui m'inquiète un peu lorsque nous parlons de la protection technologique est le fait que, dans la mesure où les entreprises jugent ces moyens de protection nécessaires, cela revient, pour moi, à mettre en accusation notre système juridique tout entier. Si notre système était à la hauteur, ces moyens ne seraient pas nécessaires. Les programmeurs ne devraient pas passer tout leur temps à essayer de rendre leurs programmes impénétrables.

Nous en arrivons maintenant aux mesures de protection offertes par la loi. Il y a immédiatement une différence naturelle entre le droit criminel et le droit civil, le droit civil couvrant essentiellement les brevets, les droits d'auteur et les procédés commerciaux secrets. En revanche, le droit criminel, pour les gens auxquels j'ai affaire, c'est-à-dire les entreprises qui oeuvrent dans ce secteur, ne représente pas la solution idéale lorsqu'il s'agit de protéger les logiciels.

La raison en est que le droit criminel est essentiellement pénal. Une entreprise à laquelle on a dérobé un logiciel se fiche pas mal des peines et des sanctions, car elle veut une récompense. Le droit criminel n'est donc pas une solution au problème de l'entreprise. Dans l'optique d'une entreprise, le droit criminel est une approche hautement inefficace.

Par exemple, dès qu'on a saisi la police ou le ministère public de l'affaire, on n'a plus aucun contrôle. Si, pour parler en termes courants, j'accuse quelqu'un, si je vais au poste de police pour demander aux représentants de l'ordre de procéder à une inculpation, si je vais trouver le procureur de la Couronne, c'est le ministère public qui prend la suite. Je n'ai plus rien à voir dans l'affaire. Peut-être serais-je cité à comparaître comme témoin, mais il m'est impossible d'aller voir le ministère public pour lui dire que j'ai changé d'avis et que je ne veux plus de poursuites judiciaires. Par conséquent, si le coupable vient me voir, vient s'excuser et vient m'offrir de me rembourser, il m'est impossible de retirer ma plainte, car seule la Couronne peut le faire. Le système n'est pas souple: il est impossible d'arriver à un règlement négocié.

L'entreprise répugne donc à porter plainte au pénal, parce qu'elle n'y a pas vraiment intérêt. Je pourrais ajouter que c'est également le public dans son ensemble qui en subit les conséquences, dans la mesure où les poursuites au pénal sont extrêmement coûteuses. Ainsi, dans un cas précis, nous avions demandé une inculpation, et un pauvre agent de la GRC a passé six mois sur le dossier, à plein temps, je crois, mais je n'en suis pas sûr. Le problème, donc, des inculpations au pénal est cette absence de souplesse, en plus du fait que la personne lésée ne peut pas retirer sa plainte.

[Texte]

Second, what happens is, when this goes to court, it is a Crown attorney who deals with it. Now, Crown attorneys are generalists; they have to deal with a number of different types of cases. They are not specialists in computer law. The accused, if he is smart about the thing, will represent himself by somebody who is a specialist, and that specialist is going to run rings around the poor Crown attorney, because the Crown attorney simply will not know all the intricacies and he can easily be bamboozled, not because of any lack of intelligence on his part, but just plain lack of specialization and knowledge in this field. The net result is that on very many of these things, if they ever do go to trial, the Crown will lose on one or other technical ground.

There is a third problem with criminal law. I started by saying that criminal law is supposed to be a deterrent; but the trouble is, if you look at the type of sentences usually given in cases dealing with commercial fraud or commercial bad behaviour of some sort, they are minimal. There may be a fine. There may be a very token prison sentence. But the reason for that, of course, is that a judge is not as shocked by something where a company has lost information as he would be if somebody had been murdered or somebody had been violently robbed or something of this sort. So the deterrence aspect of the criminal law in this field is not large.

• 1625

Therefore for these three reasons—first, no flexibility, no possibility of settlement; second, Crown counsel not being experts; third, the deterrence not being very large, because of the type of sentences—I really do not see that criminal law is of much use to a company that is looking at how to protect its data or its software.

So that leaves us with civil law, or actions between parties. I would like to give you just two basic principles of law here which really are the foundation of this.

First—and this is contrary to the intuitive idea that people have—at law you have no intrinsic right to something you create. The mere fact that you create it does not give you any right to it. That is a basic principle of law: that you do not have an intrinsic right just because you created something. The next thing that follows from that is that there is no intrinsic obligation on anybody else not to copy what you came up with.

So if there were no other principles, you would come up with something and anybody would be free to use it right away, or to copy it. Whatever rights do exist have to come from some principle of common law or some statute. So we look for what principles of common law or what statutes apply to this.

The first one that is normally used is trade secrets. That is a part of common law. It applies only where there is something

[Traduction]

En second lieu, lorsque le tribunal est saisi de l'affaire, c'est un procureur de la Couronne qui s'en charge. Les procureurs de la Couronne sont des généralistes qui doivent s'occuper d'une foule de dossiers, dans des sujets extrêmement différents. Ces gens ne sont pas des experts en matière de droit informatique. En revanche, l'accusé, s'il est tant soit peu malin, va se faire représenter par un avocat qui est, lui, spécialiste et qui va mettre le pauvre procureur de la Couronne dans sa poche, car ce dernier ignore effectivement toutes les subtilités de la chose; il peut facilement se faire jeter de la poudre aux yeux, non pas par manque d'intelligence, mais simplement parce qu'il n'est pas spécialiste, ou parce qu'il ne connaît pas le domaine. En fin de compte, dans bien des cas, lorsque les tribunaux en sont saisis, il arrive très souvent que la Couronne soit déboutée pour l'une ou l'autre raison d'ordre technique.

Le droit criminel pose également un troisième problème. J'ai dit au début que le droit criminel était censé avoir un effet de dissuasion; toutefois, l'ennui, c'est que cet effet de dissuasion est parfaitement minime, à en juger d'après les peines qui sont généralement prononcées dans les cas de fraude commerciale ou de manquement à l'éthique commerciale. C'est peut-être une amende. C'est peut-être une peine de prison de principe. Pourquoi? Parce que, bien sûr, le juge n'est pas aussi outré par le fait qu'une entreprise a perdu des données que par un meurtre, un assassinat, un vol avec violence ou un autre délit de ce genre. Dès lors, l'aspect dissuasif du droit criminel est tout à fait minime dans ce domaine.

Pour ces trois raisons donc, la rigidité, qui ne permet pas de règlement à l'amiable, le fait que les procureurs de la Couronne ne sont pas des experts et en troisième lieu le fait que l'élément de dissuasion est relativement minime compte tenu des peines infligées, je ne considère pas vraiment que le droit criminel soit très utile pour une entreprise soucieuse de protéger ses logiciels ou ses dossiers.

Il nous reste donc le droit civil ou les interventions entre parties. J'aimerais simplement vous faire part de deux principes de droit tout à fait fondamentaux qui sont à la base de tout.

En premier lieu, et ceci va totalement à l'encontre de l'opinion très intuitive que se font la plupart des gens, en droit, aucune création ne donne lieu à un droit intrinsèque. Si vous créez quelque chose, cela ne vous donne pas pour autant un droit. Voilà un principe de droit absolument fondamental: le simple fait de créer quelque chose ne vous donne aucun droit intrinsèque. Il en découle automatiquement que personne n'a l'obligation intrinsèque de s'abstenir de copier quelque chose que vous avez inventé.

En l'absence, donc, de tout autre principe, vous découvrez quelque chose et n'importe qui est libre de l'utiliser immédiatement ou de le copier. S'il y a droit, ce droit doit découler d'un principe de *common law* ou d'une loi. Nous nous demandons donc quels sont les principes de la *common law* ou les lois applicables.

Il y a en premier lieu la notion des secrets commerciaux qu'on utilise communément. Cette notion fait partie de la

[Text]

that is secret and that is kept secret. So to protect something with trade secrets, you have to start with a secret existing and with the person who has that secret taking reasonable steps to keep it secret. Then, if he does those things and he passes on the secret to somebody in confidence, in a confidential relationship, the courts are going to protect him if that person to whom he passes it on breaches confidence.

For example, if you pass on your secret in confidence to your employees because they need it to do their work, they will not be allowed to steal and sell it to somebody else. If you pass it on to another company so that that company can do some work for you, that company will not be able to steal it. But the protection given is only against the person who received that information in confidence from you; or sometimes if he passes it on to somebody else, you can sometimes nab that other person to whom he passed it on. But it is a very limited sort of protection.

Although it is limited, I must say it is very useful. It works quite well in Canada at the moment. Despite the fact that trade secrets are common law, most of the provinces of Canada are quite remarkably unified in the way they interpret trade secret law. Furthermore, in Quebec there is a Civil Code section which is again quite similar in the way it is interpreted to the common law.

So we have a fairly unified body of law across Canada in trade secrets, which is good; I am very pleased that exists. But I have to say that trade secrets are of limited use, because of what I told you before, that they apply only to secrets and to things that are given out in confidence to somebody.

• 1630

So let us take a look at the two sort of extreme circumstances where you have software that you want to protect. Suppose you have a program that has only 10 possible users and you are going to license each one of them for \$50,000 each. So it is a big program; and there are a lot of those around actually, things in particular industries where there is a very limited number of users. Now, at \$50,000 a shot, you can be sure that the parties are going to negotiate the licence very carefully and each one is going to be willing to sign a written contract and so on. In that written contract you have the statement that it is a trade secret, you have the statement that it is given in confidence and you have certain restrictions on what the person receiving it can do. That is fine. That will be protected in any court in Canada as a trade secret, and everybody will be reasonably happy with that sort of protection.

[Translation]

common law. Toutefois, elle ne s'applique que lorsque quelque chose est effectivement secret et qu'il le reste. Dès lors, pour pouvoir protéger quelque chose sous couvert du secret commercial, il faut partir d'un secret existant et il faut également que la personne qui détient ce secret prenne toutes les mesures raisonnables pour le conserver. Si c'est ce que cette personne fait et si elle met dans le secret quelqu'un en qui elle a confiance, dans le cadre de certains rapports à titre confidentiel, les tribunaux vont effectivement protéger la personne en question si celui à qui elle a communiqué le secret a abusé sa confiance.

Par exemple, vous communiquez votre secret en toute confiance à vos employés parce qu'ils en ont besoin pour travailler; à ce moment-là, ces employés ne peuvent pas vous voler votre secret et le revendre à quelqu'un d'autre. Si vous transmettez votre secret à une autre entreprise pour lui permettre de travailler pour vous, cette entreprise ne pourra pas vous voler votre secret. Toutefois, la protection accordée se limite à la personne à qui vous avez communiqué la chose sous le sceau du secret; il arrive parfois que si cette personne transmet à son tour votre secret à un tiers, vous puissiez vous retourner avec succès contre le tiers en question. Il n'en reste pas moins que c'est une protection extrêmement limitée.

Mais même si elle est limitée, elle n'en reste pas moins très utile. Au Canada, pour l'instant le système marche très bien. Même si les secrets commerciaux relèvent de la *common law*, la plupart des provinces canadiennes font assez remarquablement front commun lorsqu'il s'agit d'interpréter le droit relatif aux secrets commerciaux. Qui plus est, le Québec a dans son code civil un article qui ressemble de très près à l'interprétation usuelle des dispositions correspondantes de la *common law*.

Dès lors, sur tout le territoire canadien, nous pouvons dire que nous avons un corpus juridique relativement unifié, ce qui est parfait et j'en suis très heureux d'ailleurs. Je dois toutefois ajouter que les secrets commerciaux ont une portée relativement limitée, comme je vous l'ai dit précédemment, dans la mesure où c'est une notion qui s'applique aux secrets et à tout ce qui est communiqué à des tiers sous le sceau du secret.

Examinons de plus près ces deux genres de circonstances extrêmes, où vous avez du logiciel que vous voulez protéger. Supposons que vous avez un programme dont seules dix personnes pourront se servir, et vous allez leur vendre à chacune un permis qu'elles devront payer \$50,000. Il s'agit donc d'un gros programme, et il en existe beaucoup à l'heure actuelle. Il y a justement des programmes très particuliers, qui existent dans certaines industries, et pour lesquels le nombre d'utilisateurs est très restreint. Pour \$50,000, vous pouvez être certain que les parties intéressées vont vouloir négocier l'affaire de façon sérieuse et qu'elles vont vouloir signer un contrat, etc. Dans ce contrat écrit, vous allez stipuler qu'il s'agit d'un secret de fabrication, que les abonnés devront le garder confidentiel et que vous allez leur imposer un certain nombre de restrictions. Cela est très bien. Ainsi, votre secret de fabrication pourra être défendu devant n'importe quel tribunal

[Texte]

The problem arises on the other extreme though, where you have a video cassette or a small program for a micro-computer that you sell for \$29.95 down at one of the stores on O'Connor Street and you sell 10,000 or 20,000 copies. Nobody is going to call that a trade secret because here you have given out 20,000 copies, you have no signed agreements with the people whom you have given them out to, and so on. So trade secrets do not really work to protect that type of program where there is a large number of copies that are sold over the counter so to speak. There has been an attempt to protect that kind of program with trade secrets by what is called label licences. You see, a lot of these programs are sold in a cassette that is sealed in cellophane, and there is a little notice on it saying that this is a trade secret. You agree it is a trade secret if you break the cellophane. It is a try. It may even work in some cases, but it is very dubious. So that is about all you can do with trade secrets.

Mr. Beatty: Is that enforced by the same people who get you if you rip the label off your mattress?

Mr. Fisk: Yes, something like that. This would be enforced, though, by the owner of the company. One way that people do try to protect themselves against copying of \$29.95 cassettes is they sell them at such a low price that it is not worth the while of anybody else to make a large number of copies. It is far simpler just to go and buy one.

Another problem is that if you get a piece of information, a computer program, from somebody, how do you tell whether that is a trade secret that has been stolen? To take Professor Hammond's analogy of his chicken, suppose you are given a chicken sandwich. Do you have to inquire what coop the chicken came from? There is a limit to how far you can inquire, and yet you have here two innocent people: one person is buying the program, is innocent, and has no knowledge that it is stolen; you have also an innocent person who has had the program stolen from him. What is the poor court going to do? It has to decide which of these two innocent people should be protected. So you do have that problem too, that trade secrets work fairly well when there is a clear confidential relationship, but if somebody comes in off the street and offers you a program, you cannot really tell whether it is stolen or not.

The next thing that can be used is patents. They are a fairly good form of protection because they can be enforced against anybody who uses the patented invention in Canada, so you do not have to worry about a confidential relationship. They give quite a broad scope of protection, and are valid for 17 years. Now, there is a difference of opinion as to whether patents

[Traduction]

du pays, et tout le monde sera plus ou moins satisfait de ce genre de protection.

Un problème se pose cependant dans la situation qui correspond à l'autre extrême; vous avez par exemple une vidéocassette ou un petit programme pour micro-ordinateur que vous vendez pour \$29.95 dans l'un des magasins de la rue O'Connor. Vous en vendez peut-être 10,000 ou 20,000 exemplaires. Personne ne considérera cela comme étant un secret de fabrication, car vous aurez distribué 20,000 copies de votre programme, vous n'aurez signé aucun contrat avec ces gens-là, etc. La loi sur les secrets de fabrication ne pourra pas vraiment protéger ce genre de programme lorsqu'il est vendu en grand nombre à toutes les personnes qui se présentent au comptoir du magasin. On a essayé de protéger ce genre de programme avec ce que l'on appelle des permis d'étiquette. Voyez-vous, bon nombre de ces programmes sont vendus sous forme de cassettes enveloppées de cellophane, et il y a dessus une petite étiquette qui dit qu'il s'agit d'un secret de fabrication. Il est convenu que dès que vous déchirez la cellophane, vous êtes en possession d'un secret de fabrication. C'est une tentative de protection. Cela peut fonctionner dans certains cas, mais c'est assez douteux. C'est à peu près tout ce que vous pouvez faire pour ce qui est des secrets de fabrication.

M. Beatty: Et le respect de ces règles est-il assuré par les mêmes personnes qui vous font des ennuis si vous arrachez l'étiquette de votre matelas?

M. Fisk: Oui, en quelque sorte. Mais ce serait imposé par le propriétaire de la société. Une façon dont les gens essaient de se protéger contre la reproduction de ces cassettes à \$29.95, c'est qu'ils les vendent à un prix si bas qu'il n'est vraiment pas intéressant pour quelqu'un d'essayer de les reproduire en grand nombre. C'est plus simple de tout simplement aller s'en procurer une autre au magasin.

Un autre problème, c'est que si vous obtenez certains renseignements ou un programme informatique auprès de quelqu'un, comment pouvez-vous savoir s'il s'agit d'un secret de fabrication qui a été volé? Pour reprendre l'analogie avec le poulet qu'a cité le professeur Hammond, supposons qu'on vous donne un sandwich au poulet. Êtes-vous tenu de vous renseigner pour savoir d'où provient le poulet? Il y a une limite jusqu'où peuvent aller vos enquêtes, et pourtant, il y a là deux personnes innocentes: celle qui achète le programme est innocente, elle ne sait pas que celui-ci a été volé; et celle qui s'est fait voler son programme est également innocente. Que va donc faire le tribunal? Il aura à décider laquelle de ces deux personnes innocentes devrait être protégée. Il y a donc cet autre problème: l'histoire des secrets de fabrication marche assez bien lorsqu'il y a des relations confidentielles clairement établies, mais si quelqu'un entre dans votre boutique et vous offre un programme, vous ne pouvez pas savoir s'il a été volé ou non.

On peut également recourir aux brevets. Il s'agit là d'une assez bonne formule de protection, car ces brevets doivent être respectés par quiconque se sert de l'invention brevetée au Canada; il n'est donc plus nécessaire de s'intéresser à des relations confidentielles. Ces brevets donnent une protection assez vaste et sont valables pour une période de 17 ans. Mais

[Text]

should apply to computer programs. In most European countries they have passed legislation to say that patents should not apply to computer programs. In the United States, however, they have gone the other way. The court cases have said that computer programs can be inventions like any other type of invention. Therefore, the same criteria of patentability should apply to them.

• 1635

There is one reason why the Europeans went the way of saying that computer programs should not be protected by patents. This is because under most patent systems, before a patent is granted, it is examined by the government to see that it meets certain criteria, to see that it is new, it is useful and it is an obvious. Now, a good many of the European countries said to themselves: If we examine all these patent applications on computer programs, we will have to hire skilled computer programmers for our patent offices; and we do not have enough computer programmers to go around already, so it is going to be very difficult to examine these patents. And that is a problem. It is a problem that the United States is meeting, but it is a problem you have to recognize.

In Canada, our legislation is silent on computer programs. That is not really surprising since our Patent Act was created in 1935, and it has not really been substantively amended since, except on one minor matter in 1969 dealing with drugs. Really, there is no indication in the legislation whether computer programs should be included.

There is, however, one case in Canada which went to the Federal Court of Appeal, and in that one the court said that the particular computer program involved was not patentable because it was for a mere scientific principle or abstract theorem. Now, I disagree with the ruling of the court, and I would love to get before them with a proper case and see if we could change it; but at the moment the way things stand, it would appear that computer programs are not patentable in Canada, and the Patent Office following the lead of the court has been refusing program patents.

My own view as to whether computer programs should be patentable in Canada, I think you should approach this with some caution, because patent protection can be very broad. If you have a thicket of patents, and everybody has a patent on some area of programming, you may inhibit the development of the industry; but there is a good side too. One of the reasons for patenting is that the government may give a short-term monopoly, but it gets in return a full disclosure of the invention, so even though a monopoly is given for a period of time, that gets disclosed and other people can look at it and can have ideas that derive from it.

[Translation]

tout le monde n'est pas d'accord pour dire que des brevets devraient exister pour des programmes d'ordinateur. Dans la plupart des pays européens, on a adopté des lois disant que les brevets ne devraient pas s'appliquer aux programmes informatiques. Aux États-Unis, par contre, ils sont allés dans le sens inverse. Là, les tribunaux disent que les programmes informatiques peuvent être des inventions au même titre que n'importe quelle autre invention. Par conséquent, le même critère devrait s'appliquer à eux pour ce qui est de l'obtention de brevets.

Il y a une raison pour laquelle les Européens ont décidé de dire que les programmes informatiques ne devraient pas être protégés par des brevets. C'est parce que, dans le cadre de la plupart des systèmes, avant qu'un brevet ne soit accordé, l'invention est examinée par le gouvernement, pour vérifier si elle satisfait à certains critères, s'il s'agit de quelque chose de nouveau, d'utile et d'une utilisation évidente. Les gens, dans beaucoup de pays européens, se sont donc dit: si nous examinons toutes les demandes de brevets pour des programmes informatiques, il nous faudra embaucher des programmeurs très qualifiés; or, il n'y a déjà pas suffisamment de programmeurs; alors, il nous serait vraiment très difficile d'examiner toutes ces demandes. C'est un problème. C'est un problème que les Américains ont décidé de résoudre, mais c'est néanmoins un problème.

Les lois canadiennes passent sous silence les programmes informatiques. Cela n'a vraiment rien d'étonnant, puisque la Loi sur les brevets remonte à 1935, et elle n'a pas été beaucoup modifiée depuis, à l'exception d'une question mineure au sujet des stupéfiants, qui y a été incorporée en 1969. La loi ne dit aucunement si les programmes informatiques devraient y être inclus ou non.

Il y a cependant une affaire, au Canada, qui a été portée devant la Cour d'appel fédérale. La cour avait décidé que le programme informatique concerné n'était pas brevetable, parce qu'il ne s'agissait que d'un principe ou d'un théorème abstrait scientifique. Je ne suis pas d'accord avec la décision rendue par la cour, et j'aimerais pouvoir la saisir d'une affaire solide, pour voir s'il ne serait pas possible de changer les choses. Mais, à l'heure actuelle, il semblerait que les programmes informatiques ne soient pas brevetables au Canada, et le Bureau des brevets suit l'exemple donné par la cour, en refusant de breveter les programmes informatiques.

Quant à mon avis personnel sur la question de savoir si les programmes d'ordinateur devraient être brevetables au Canada, je pense qu'il faut faire preuve de prudence, parce que la protection accordée par des brevets peut être très vaste. Si tout le monde a un brevet pour un domaine donné de la programmation, il y en aura bientôt tout un tas, et il se peut que cela entrave le développement de l'industrie; mais il y a également l'aspect positif de la chose. L'une des justifications de l'octroi de brevets, c'est que le gouvernement pourrait autoriser un monopole à court terme, mais il recevrait en retour une divulgation de l'invention. Ainsi, même s'il y avait un monopole pendant une période de temps donné, les

[Texte]

Therefore, in an emerging industry like the computer industry, it does not benefit the industry if everybody keeps their little advances secret. So the patent system at least gets the advances out in the open. It gives people the confidence to disclose those advances in return for a period of protection. On balance, I would say that patent protection is useful, but I would also say that it is important when you are considering patent protection for the computer industry to make sure that there are high standards before you get a patent, particularly high standards of unobviousness, so that you do not have all sorts of little patents that just bother the industry and block them from doing things they should do.

The last form of protection that you can use in the computer industry is copyright. Now most industrialized countries have permitted protection of computer software by copyright. In fact, in the United States, they did an amendment to their copyright act in 1978 to specifically include computer programs, and this was after a thorough study by the President's committee on new technological uses, which is generally known as CONTU. So there was a thorough study of it, and then they made an amendment to their copyright act saying that computers should be protected by copyright.

• 1640

We are a little out of step on this one. We have a Copyright Act that comes from 1921, really. The act was passed in 1921, effective 1924. Of course, there were not many computer programs around at that time—it was based on a 1911 act—so our act does not say anything about computer programs. There was some doubt whether it applied, because, for example, you have to fit it into certain categories in the act, and we had some trouble fitting computer programs into these categories. Everybody was reasonably sure, however, that computer programs were covered by copyright. Then, along came a rather shocking case, this past December. The judge involved, incidentally, was an ex-Speaker of this House. The judge refused to grant an interlocutory injunction in a case where there was clearly copying. The reason they can say there was clearly copying was that the alleged infringer not only copied the program, but within the program he copied a data loop which said "Property of Atari Corporation", so the infringement included a statement indicating who was the creator of the program.

The judge, however, refused to grant an interlocutory injunction because he said that there was some doubt whether the present Canadian Copyright Act covers computer programs. So we have this problem that there is that decision, and

[Traduction]

renseignements seraient éventuellement divulgués, et d'autres gens pourraient les examiner et en dériver de nouvelles idées.

Dans une industrie encore naissante, comme l'est celle de l'informatique, ce n'est guère avantageux pour elle que chacun garde ses inventions et ses progrès dans le secret le plus total. Un système de brevets permet au moins de tenir les gens au courant. Et cela donne aux gens suffisamment de confiance pour qu'ils veuillent divulguer leurs découvertes, puisqu'on leur donne, en retour, une certaine période de protection. À tout prendre, je dirais que la protection que donnent les brevets est utile, mais je m'empresserai de préciser qu'il est très important, dans le contexte de l'industrie de l'informatique, de veiller à ce que des normes très élevées soient imposées, et je songe en particulier aux normes relatives aux critères de l'utilité évidente ou manifeste, sans quoi vous vous retrouverez avec tout un tas de petits brevets qui entravent l'industrie et qui l'empêchent de faire ce à quoi elle devrait se consacrer.

La dernière forme de protection à laquelle on puisse recourir dans le domaine de l'informatique, c'est le droit d'auteur. La plupart des pays industrialisés ont permis la protection du logiciel informatique grâce aux droits d'auteur. D'ailleurs, les Américains ont modifié, en 1978, leur loi sur les droits d'auteur, afin que celle-ci s'applique aux programmes informatiques. Cette décision a été prise suite à une étude approfondie réalisée par le comité du président sur les nouvelles technologies, connu sous le nom de CONTU. On a donc étudié la question de très près, après quoi la loi sur les droits d'auteur a été modifiée, afin qu'il soit clairement stipulé que les ordinateurs pouvaient être protégés par des droits d'auteur.

Nous avons un léger retard sur ce plan-là. Nous avons une Loi sur le droit d'auteur qui remonte en fait à 1921. La loi fut adoptée en 1921, mais elle n'est entrée en vigueur qu'en 1924. Évidemment, à cette époque-là, il n'y avait pas beaucoup de programmes informatiques—le texte a été préparé à partir de celui d'une loi de 1911—alors, la loi ne dit rien au sujet des programmes informatiques. On n'était pas certain que la loi s'y appliquait, parce qu'on a eu du mal à insérer les programmes informatiques dans l'une ou l'autre des catégories qui sont définies dans la loi. Tout le monde était cependant plus ou moins certain que les programmes d'ordinateur étaient couverts par le droit d'auteur. Mais en décembre dernier, il a été question d'une affaire assez surprenante. Le juge qui en avait été saisi était, je le souligne en passant, l'ancien Orateur de la Chambre. Le juge a refusé d'accorder une injonction interlocutoire pour une affaire où il y avait clairement eu reproduction. Et s'il est possible d'affirmer qu'il y a eu reproduction, c'est que l'accusé a non seulement copié les programmes, mais il a copié, au sein de celui-ci, une boucle qui disait «propriété de la société Atari». Sa reproduction comprenait donc même une déclaration indiquant qui avait créé le programme.

Le juge a cependant refusé d'accorder une injonction interlocutoire, parce qu'il a dit qu'il n'était pas certain que la Loi sur le droit d'auteur, dans son libellé actuel, couvrait les programmes d'ordinateur. Cette décision ayant été rendue,

[Text]

now we are a little bit worried. We have been relying happily on copyright up until now, but I have to admit that it is difficult to fit computer programs into the square wording of the act, and we now have a judgement which casts some doubt on whether computer programs are fitted in.

Otherwise, copyright is a fairly good form of protection; it is narrower than patents; it does not block other people from the field because copyright only protects against copying. Therefore, if you develop it independently, you do not infringe copyright.

One problem with copyright is that it is a fairly long period of protection, though. It is life of the author plus 50 years.

My recommendations on copyright are, first, that I think it is a matter of urgent priority that the Copyright Act be amended to make it clear that copyright applies to computer programs and to data held in electronic form in a computer. You see, at the moment, it would appear that in order to have copyright on something, there has to be a hard copy form. If the data is held just in electronic impulses in a computer, there is no copyright in that data. I would therefore say that it is important to amend the Copyright Act to make it clear that it applies to computer programs and to data held in electronic form in a computer.

You should also make it quite clear that the copyright applies, no matter what form the data is in, because it could be on a memory board, a read-only memory, or ROM, as they are called, or it could be in source code, or in object code; it could be on tape; it could be on disc; it could be on a drum; it could be in many ways. Therefore it is important that whatever amendment there is, it be very broad to cover the programs no matter what form they are in.

I do think that life plus 50 years is fairly long. I do not think that is necessary for the protection of computer programs, because programs have a fairly short lifespan these days. Possibly it is necessary, or desirable, with respect to data, so I think we might make a distinction there, that perhaps programs get a shorter period of protection, and I would say that 15 years is probably reasonable, and data possibly 50 years.

Remember I said that a program normally was protected for the life of the author plus 50 years. You may have great fun in computer programs figuring out who the author is, particularly now that we have some programs that can write other pro-

[Translation]

cela pose un problème qui nous préoccupe quelque peu. Nous comptons jusqu'alors sur le droit d'auteur, mais je dois avouer qu'il est difficile de caser les programmes informatiques dans le libellé très précis de la loi, et cette décision dont je viens de vous parler nourrit quelques doutes dans notre esprit quant à la possibilité de faire couvrir les programmes informatiques par cette loi.

Mais si on ne tient pas compte de cela, le droit d'auteur est une assez bonne forme de protection, c'est plus étroit que les brevets; et cela ne bloque pas les autres gens qui travaillent dans le domaine, parce que le droit d'auteur n'interdit que la reproduction. Par conséquent, si vous mettez le même programme au point de façon indépendante, cela ne constitue pas une infraction.

L'un des problèmes, avec le droit d'auteur, par contre, c'est qu'il prévoit une période de protection assez longue. Cette période correspond à la vie de l'auteur, plus 50 ans.

Pour ce qui est du droit d'auteur, je dirais tout d'abord qu'en ce qui me concerne, il est très important que la Loi sur le droit d'auteur soit modifiée rapidement, afin qu'il soit bien clair que le droit d'auteur s'applique aux programmes informatiques et aux données versées sous une forme électronique dans les ordinateurs. Voyez-vous, à l'heure actuelle, il semblerait que, pour avoir un droit d'auteur pour quelque chose, il faut qu'il y ait quelque chose de tangible. Mais si les données ne correspondent qu'à des signaux électroniques dans un ordinateur, il ne serait alors pas possible d'avoir un droit d'auteur pour ces données. C'est pourquoi je dis qu'il est impératif que la Loi sur le droit d'auteur soit modifiée, afin qu'il soit clair que cette loi s'applique aux programmes informatiques et aux données qui se présentent sous une forme électronique dans les ordinateurs.

Il faut également qu'il soit clair que le droit d'auteur s'applique à ces données, quelle que soit la forme sous laquelle elles se présentent, car elles peuvent être contenues dans une planche de mémoire, dans une mémoire fixe, ou dans une mémoire morte. D'autre part, elles peuvent être exprimées sous forme de code source ou de code objet; elles peuvent être enregistrées sur bande, sur disque, ou encore sur tambour. Les possibilités sont multiples. C'est pourquoi il est important que les amendements apportés à la loi soient assez vastes pour pouvoir couvrir les programmes, quelle que soit la forme sous laquelle ceux-ci se présentent.

Je trouve que la vie de l'auteur, plus 50 ans, est une période assez longue. Et je ne pense pas que cela soit nécessaire pour protéger les programmes informatiques, car, de nos jours, la durée de vie de ces programmes est assez courte. Cela serait peut-être nécessaire ou souhaitable, par contre, pour ce qui est des données; c'est pourquoi je pense qu'il faudrait peut-être faire une distinction ici: l'on pourrait peut-être prévoir une période de protection plus courte pour les programmes, et 15 ans serait sans doute une période raisonnable, et l'on pourrait fixer cette période à 50 ans pour les données.

Souvenez-vous que j'ai dit tout à l'heure qu'en règle générale, un programme est protégé pour la vie de l'auteur, plus 50 ans. Mais il n'est pas toujours facile de trouver qui est l'auteur d'un programme donné, parce que certains programmes peuvent maintenant en créer d'autres. Allez donc savoir

[Texte]

grams. So who is the author? Is it computer number such and such?

• 1645

So I think when we deal with this, we should also make an amendment saying that it is not necessary to specify who the author is of computer programs. Perhaps all we need to say is that it was authored under the control of Company X, and therefore Company X would be the author.

Thank you very much.

The Chairman: Thank you.

Mr. Beatty.

Mr. Beatty: Thank you, Madam Chairman.

Let me first of all say that I think these were two of the most useful presentations we have had. I think the two of them are in many ways complementary in the areas we have been dealing with.

First of all, Mr. Fisk, I certainly agree with you that it appears in the protection of software probably copyright legislation is the most obvious route for us to follow. I am wondering whether you would be prepared to make some comment, though, in other areas, such as, for example, the integrity of other data held in the system which might not be copyrightable but which might be of some value to a company or to an individual and which either the institution or the individual would not want to have an unauthorized party have access to. What sort of protection do you feel the law should provide for in that instance?

Mr. Fisk: You are getting there to some extent along the same lines as the invasion of privacy statutes. I see nothing wrong with using the criminal law in that sort of arrangement, where you are using the criminal law to protect against breaking into a computer either metaphysically or physically... in other words, by electronic means or by physical means—and taking out data or manipulating data or something of that sort. I think that is something that can be protected by the criminal law. It can also be protected, of course, to some extent by the civil law, because there is what is called “nuisance” in the civil law, which is an area where you can sue somebody for, basically, doing something that harms you.

Mr. Beatty: But you would have to demonstrate harm. In the University of Alberta case, I believe charges were successfully pressed against one individual because of loss of use of the system, if I understand it correctly. But in an instance where I simply gained unauthorized access to your files and where I did not damage you in any tangible way and simply copied the information in there, you would not have any recourse under the law at the present time.

Mr. Fisk: Actually, you would under copyright. There have been some strange cases. Copyright has been stretched to some

[Traduction]

qui en est l'auteur. Il peut très bien s'agir de l'ordinateur numéro un tel.

C'est pourquoi je pense qu'il conviendrait d'y apporter un amendement qui dit qu'il n'est pas nécessaire de préciser qui est l'auteur des programmes informatiques. Il suffirait peut-être de dire que tel programme a été créé sous l'égide de la société X, et que la société X doit par conséquent être considérée comme étant l'auteur.

Merci beaucoup.

Le président: Merci.

Monsieur Beatty.

M. Beatty: Merci, madame le président.

Permettez-moi de dire tout d'abord que ces deux mémoires ont été parmi les plus intéressants que nous ayons entendus. D'autre part, je pense qu'ils se complètent très bien tous les deux dans les domaines qui nous intéressent ici.

Tout d'abord, monsieur Fisk, je suis d'accord avec vous pour dire qu'il semblerait que la meilleure solution pour protéger le logiciel est sans doute de recourir à la Loi sur le droit d'auteur. Mais je me demande si vous pourriez faire quelques commentaires au sujet d'un certain nombre d'autres questions, comme l'intégrité d'autres données contenues dans un système, données qui ne pourraient peut-être pas faire l'objet d'un droit d'auteur, mais qui pourraient revêtir une certaine valeur pour une société ou pour un particulier qui ne souhaiteraient pas que des personnes non autorisées y aient accès. Selon vous, quel genre de protection la loi devrait-elle offrir dans ce genre de situation?

M. Fisk: Le problème que vous abordez là rejoint, dans une certaine mesure, la question de l'empiètement sur le droit à la protection de sa vie privée. Je ne vois rien de mal à recourir au droit pénal dans ce genre d'arrangement, où vous vous servez du droit pour assurer une protection contre la violation d'un ordinateur, que ce soit métaphysiquement ou physiquement—autrement dit, en recourant des moyens électroniques ou physiques—et le vol ou la manipulation de données. Je pense que c'est là quelque chose qui pourrait être protégé par le droit pénal. Ce pourrait également être bien protégé, dans une certaine mesure, par le droit civil, car il existe ce qu'on appelle le droit civil des actes préjudiciables. Vous pouvez intenter un procès contre quelqu'un qui a fait quelque chose qui vous a nui.

M. Beatty: Mais il faudrait pouvoir démontrer qu'il vous a nui. Dans l'affaire de l'Université de l'Alberta, si je me souviens bien, on a réussi à obtenir l'accusation de l'une des personnes, parce que ses actes avaient amené une perte de l'utilisation du système. Mais si j'avais, sans en avoir obtenu l'autorisation, eu accès à vos dossiers, et si je ne vous avais pas nui de façon tangible, si, par exemple, je n'avais fait que recopier les données contenues dans vos dossiers, vous n'auriez, à l'heure actuelle, aucun recours légal.

M. Fisk: Vous auriez un recours en vertu de la Loi sur le droit d'auteur. Il y a eu quelques affaires assez étranges. Le

[Text]

areas. For example, in England they proceeded against a reporter who had access to some Cabinet documents, on the basis that he had infringed the government copyright in those documents. So it was not what one normally considers as a copyright case, but copyright was used.

Mr. Beatty: But what if you simply read the information that was on there and did not copy it as such?

Mr. Fisk: No, there is no way of dealing with it in copyright. You would have to do it through the criminal law.

Mr. Beatty: And yet potentially it would still be a concern of the owner of the information it held.

Mr. Fisk: That is correct.

Mr. Beatty: Could I ask you to comment—I assume you agree with Professor Hammond's analysis of the various bites that we should be taking of the subject. The first issue would be the preservation of the integrity of the system itself, and that should be properly dealt with in the Criminal Code.

Mr. Fisk: Yes.

Mr. Beatty: Secondly, you could set aside a second group of concerns you could lump under the heading "improper trafficking of commercial information".

Mr. Fisk: Yes.

Mr. Beatty: Much of it would be in the civil law area; and indeed, you have offered your description in that area for what we should be doing.

Mr. Fisk: I do agree with one thing Professor Hammond said, though, which is that it may well be useful to have a criminal sanction as well, because of the extra-territorial aspect. Territorial boundaries are becoming less and less important at the moment. I routinely, for example, access a computer in Cleveland for legal information. That is becoming a perfectly normal thing to do. And if that happens, there is this problem of how you sue somebody in another jurisdiction. So criminal law is perhaps a better way of dealing with it.

• 1650

Mr. Beatty: This raises the question in my mind that, assuming we had a situation in which we had a data bank with dial-in access to it that was similar to the systems that were broken into by the Dalton school group...

Mr. Fisk: Yes.

Mr. Beatty:—and that information was copied. At the present time you would have no recourse if it were done across boundaries, even under copyright presumably?

[Translation]

droit d'auteur a été étendu, pour s'appliquer à d'autres domaines. En Grande-Bretagne, par exemple, on a intenté un procès contre un journaliste qui avait eu accès à certains documents du cabinet; on l'avait accusé d'empiéter sur le droit d'auteur du gouvernement pour ce qui est de ces documents. Il ne s'agit pas là d'une affaire typique ou classique en matière de droit d'auteur, mais on a utilisé le droit d'auteur pour porter des accusations contre le journaliste.

Mr. Beatty: Mais que se passerait-il si vous ne faisiez que lire les renseignements contenus dans ces dossiers, sans les recopier en tant que tels?

Mr. Fisk: Dans ce cas-là, il ne serait pas possible de recourir au droit d'auteur; il faudrait recourir au droit pénal.

Mr. Beatty: Or, potentiellement, cela constituerait toujours une source de préoccupations pour le propriétaire des données concernées.

Mr. Fisk: C'est exact.

Mr. Beatty: Pourrais-je vous demander de faire des commentaires... Je suppose que vous êtes d'accord avec l'analyse faite par le professeur Hammond des différents aspects de la question dont nous devrions nous occuper. La première question serait la préservation de l'intégrité du système lui-même, et cela devrait être couvert par le Code criminel.

Mr. Fisk: Oui.

Mr. Beatty: Deuxièmement, vous pourriez rassembler un certain nombre de choses dans un deuxième groupe que vous pourriez appeler «trafic impropre de données commerciales».

Mr. Fisk: Oui.

Mr. Beatty: Un grand nombre de ces questions seraient couvertes par le droit civil. D'ailleurs, vous avez déjà décrit ce que nous devrions faire selon vous.

Mr. Fisk: Je suis cependant d'accord avec l'une des recommandations du professeur Hammond: je pense qu'il serait peut-être utile de prévoir également une sanction criminelle, à cause de l'aspect extra-territorial du problème. Les frontières deviennent de moins en moins importantes. J'interroge, par exemple, régulièrement un ordinateur situé à Cleveland, et ce, pour avoir des données juridiques. Cela devient une chose tout à fait courante et normale. Et si cela continue, il se posera le problème de savoir comment poursuivre quelqu'un dans une autre juridiction. Le droit pénal serait donc peut-être une meilleure solution.

Mr. Beatty: Cela soulève une question dans mon esprit: supposons qu'il s'agisse d'une banque de données avec accès par téléphone, comme les systèmes qui ont été violés par le groupe de l'école Dalton...

Mr. Fisk: Oui.

Mr. Beatty:... et que les données ont été copiées. À l'heure actuelle, si cela se produisait dans des pays différents, vous n'auriez aucun recours, même pas en vertu de la Loi sur le droit d'auteur?

[Texte]

Mr. Fisk: Actually, you would. Copyright is an example of a great deal of international co-operation. There are two international treaties to which Canada is a member. One of them is generally called the Bern Convention. To give it its full name it is The International Convention For the Protection of Industrial Property—Copyright Aspect, and it has, I think, close to 100 countries as members at the moment. There is also the Universal Copyright Convention which has about 60 countries as members. The United States is a member of the Universal but not the Bern Convention.

Basically, what both of these conventions do is permit, if you have created something in one member country or have created by nationals of one member country, an action to be brought for infringement in any other member country according to the domestic law of that country. The Universal Copyright Convention is a little more stringent than the Bern Convention, because it requires that C within a circle that you have seen. That is where that comes from. That is a Universal Copyright Convention requirement. But, generally, copyright is one of the few international things that we have, few international protections in that if you create something in Canada and mark it correctly, in close to 100 countries you have got protection right away without doing anything else.

Mr. Beatty: Where does the offence take place?

Mr. Fisk: Where the copying occurs, or where the copy is. If the copy is physically in the United States, you can sue the person in the United States.

Mr. Beatty: Would the copying have taken place in Canada, if the data bank were in Canada, or does it take place at the other end of the phone line?

Mr. Fisk: For a copyright suit it does not really matter, because you can go after them wherever they are using the copy. But from a legal point of view I would say the copying probably takes place in the place where the figures were imprinted on the paper. But from a copyright point of view, it just does not matter.

Mr. Beatty: In Professor Hammond's first category, the preservation of the integrity of the computer system, which he would use the Criminal Code to do, what would be the nature of legislation you could see dealing with that?

Mr. Fisk: Well, it is almost analagous to the mischief statutes that we have. Mischief can be a very flexible type of law because a judge can give an absolute discharge to somebody who has set a waste basket on fire on hallowe'en night or he can give a jail sentence to somebody who has, with malice, damaged something rather serious. So it is a very flexible sort of law and I think that something analagous to that sort of provision would be appropriate here.

Mr. Beatty: Would an offence similar to computer trespass or data trespass be appropriate?

Mr. Fisk: Something along that line, sure.

Mr. Beatty: One final question before I ask Professor Hammond. He made one point which was at variance with

[Traduction]

M. Fisk: Si. Le droit d'auteur est un bon exemple de collaboration internationale. Le Canada est signataire de deux traités internationaux. L'un d'eux s'appelle la Convention de Berne. Son titre au complet, c'est la Convention internationale pour la protection de la propriété industrielle—Droit d'auteur. Je pense que près de 100 pays en sont signataires à l'heure actuelle. Il y a également la Convention universelle sur le droit d'auteur, dont 60 pays sont signataires. Les États-Unis ont signé la Convention universelle, mais non la Convention de Berne.

Voici, en gros, ce que prévoient ces deux conventions: si un pays ou les ressortissants d'un pays signataire ont créé quelque chose, et si quelqu'un d'un autre pays membre viole la convention, vous pouvez tenter des poursuites contre cette personne en vertu du droit du pays concerné. La Convention universelle sur le droit d'auteur est un peu plus stricte que la Convention de Berne, car elle exige ce «C» dans le cercle que vous avez déjà vu. C'est de cela que cela vient. C'est une exigence de la Convention universelle sur le droit d'auteur. Mais le droit d'auteur est l'une des seules choses que nous ayons négociées à l'échelle internationale; c'est l'une des rares formes de protection internationale qui existent pour protéger ce qui est créé au Canada et est employé correctement. Cette protection est assurée dans près de 100 pays, sans que vous soyez obligés de recourir à autre chose.

M. Beatty: Où est commise l'infraction?

M. Fisk: Le travail de copiage est fait là où se trouve la copie. Si la copie est physiquement aux États-Unis, vous pouvez poursuivre la personne aux États-Unis.

M. Beatty: Le copiage aurait-il eu lieu au Canada, si la banque de données était située au Canada, ou cela se déroule-t-il à l'autre bout de la ligne téléphonique?

M. Fisk: Lorsque vous invoquez le droit d'auteur, cela importe peu, parce que vous pouvez les poursuivre là où ils utilisent la copie. Mais du point de vue légal, je dirais que le copiage se déroule vraisemblablement là où les chiffres sont imprimés sur papier. Mais pour ce qui est du droit d'auteur, cela n'entre pas en ligne de compte.

M. Beatty: Pour ce qui est de la première catégorie citée par le professeur Hammond, c'est-à-dire la préservation de l'intégrité du système informatique, pour lequel il recourait au Code criminel, quel genre de loi s'appliquerait là, selon vous?

M. Fisk: C'est presque analogue aux règlements en matière d'actes préjudiciables au public que nous avons. La loi est assez souple là-dessus, parce qu'un juge peut acquitter quelqu'un qui a mis le feu à une poubelle le soir de l'halloween, et il peut recommander l'incarcération de quelqu'un qui a endommagé quelque chose avec intention criminelle. Il s'agit donc d'une loi assez souple, et il me semble que quelque chose d'analogue à cela serait tout à fait opportun ici.

M. Beatty: La violation d'ordinateurs ou de données serait-elle une infraction à propos?

M. Fisk: Quelque chose du genre, oui.

M. Beatty: J'aimerais vous poser une dernière question avant de m'adresser au professeur Hammond. Il a fait une

[Text]

some other testimony we had, and he quite properly anticipated we would have had this testimony. That was the recommendation that there should be a positive legal onus put upon the institution to maintain proper security standards. Both yesterday and also when Professor Flaherty from the University of Western Ontario came, the argument was made that institutions have a responsibility to maintain proper standards of security in the system themselves and that might particularly be the case where an institution had information about me.

Mr. Fisk: Yes.

Mr. Beatty: For example, credit records or other information where there might or might not be any actual financial injury to me if the information were to get out but where I would feel my privacy was invaded. My medical record might be another case. Do you feel there should be legislation that imposes a positive onus on institutions to maintain proper security standards for this sort of information?

• 1655

Mr. Fisk: For sensitive information, yes, I think there should be. In fact, in some ways there is. If you look at the credit reporting acts of the provinces, for example, there is an onus to not give out information beyond certain accepted areas. I would think that for this type of information, there should be some sort of onus. This is not the type of information that I was dealing with particularly in my talk. I was dealing with something more along the lines of something which is of value and can be sold or licensed. I was dealing with it more in terms of the company who owns it, protecting it so that somebody else will not get to the public and sell it before they get to the public and sell it. But as to the type of information that you were talking about, yes, I consider there should be some limitation on its use.

Mr. Beatty: Probably on a case-by-case basis in terms of the category of information and not . . . The recommendation was made, I believe, yesterday that, for example, companies which do business with the federal government either to receive grants or to receive contracts from the federal government could have . . . As a condition of contract in each instance, it would be written in that there be appropriate security measures taken. You, I gather, would be more inclined to deal with things on an ad hoc basis rather than the federal government going with a broad sweep and saying that across the board we are going to have some data protection standards which must be met.

Mr. Fisk: With respect to whoever made that presentation to you, I think it would be terribly counterproductive because much of this data should be available to the public. There is a lot of information generated as a result of government contracts which is of public use and which neither the com-

[Translation]

remarque qui va à l'encontre de ce qui a été dit par un certain nombre d'autres témoins que nous avons rencontrés, et il avait justement prévu que cela aurait été le cas. J'aimerais faire ici allusion à sa recommandation voulant que l'institution soit tenue, de par la loi, de maintenir des normes de sécurité adéquates. Hier, et également lors de la comparution du professeur Flaherty, de l'Université Western Ontario, il a été dit que les institutions avaient pour responsabilité de maintenir des normes de sécurité adéquates elles-mêmes, et que ce serait tout particulièrement le cas lorsque les institutions concernées auraient des renseignements à mon sujet, par exemple.

M. Fisk: Oui.

M. Beatty: Par exemple, des renseignements sur mes possibilités de crédit, ou d'autres données qui pourraient ou qui ne pourraient pas me nuire financièrement, si ces renseignements étaient divulgués, mais pour lesquels je pourrais avoir le sentiment que ma vie privée a été violée. Mes dossiers médicaux seraient un autre exemple. Pensez-vous qu'il faille avoir une loi qui impose aux institutions l'obligation de maintenir des normes de sécurité adéquates pour protéger ce genre de renseignements?

M. Fisk: Oui, je pense que ce devrait être le cas lorsqu'il s'agit d'information délicate. En fait, de certaines façons, cela existe. Si vous regardez, par exemple, les lois provinciales sur la divulgation de renseignements relatifs au crédit, vous avez la responsabilité de ne pas divulguer de renseignements en dehors de certaines limites acceptées. Je pense que pour ce type de renseignement il devrait y avoir un genre de responsabilité. Ce n'est pas de ce genre de renseignement que je parlais dans mon exposé. Je parlais plutôt de renseignements de valeur, qui peuvent être vendus ou faire l'objet d'un brevet. Je traitais de la question plutôt du point de vue de la compagnie détenant ces renseignements, du point de vue de la protection de ces renseignements afin d'éviter que quelqu'un d'autre s'en accapare et les vende au public avant que la compagnie elle-même puisse le faire. Toutefois, pour le type de renseignement dont vous parlez, oui, je pense qu'il faudrait en quelque sorte en limiter l'utilisation.

M. Beatty: Probablement en procédant cas par cas selon la catégorie de renseignement et non . . . Hier, par exemple, on a recommandé que les entreprises transigeant avec le gouvernement fédéral, qui en reçoivent des subventions ou des contrats, pourraient avoir . . . Dans chaque cas, l'une des conditions du contrat pourrait être que l'on prenne des mesures de sécurité suffisantes. Si j'ai bien compris, vous auriez plutôt tendance à régler les choses au fur et à mesure que de voir le gouvernement fédéral prendre des grandes mesures en disant à tout le monde que désormais il y aura des normes de protection des données qu'il faut respecter.

M. Fisk: Sans manquer de respect à quiconque vous a fait cet exposé, je pense que cela aurait des inconvénients car le public devrait avoir accès à une bonne partie de ces données. Une grande partie de l'information découlant des contrats du gouvernement est d'utilité publique et ni les compagnies ni le

[Texte]

pany nor the government has any reason to protect. For example, there are companies that do weather research for the Canadian government. The whole purpose of this research is to make information available so that people in universities and research institutes and so on can use it and possibly come up with some ideas as to how the weather can be forecast better. I think any sweeping provision that would say that all data generated in respect of government contracts should be secret would be very counterproductive. I would guess that well over half the information does get out somehow and quite happily gets out. I could think on this particular field we are talking about now; there have been several position papers prepared, which are under contract to the Canadian government by various people, on amendments to the Patent Act and amendments to the Copyright Act. By this sweeping provision, all of these would be secret. Actually, I am trying to get my hands on as many as possible because I want to be able to predict what the government will do.

Mr. Beatty: Thank you, Mr. Fisk.

Professor Hammond, you talked about creating two offences, one for unauthorized use and the other for, in essence, meddling with data.

On the first one, unauthorized use, would an offence similar to data trespass be appropriate there? Or computer trespass—unauthorized access, in essence?

Mr. Hammond: This is sort of a cohesive concept which I think has found favour, particularly in some of the Scandinavian countries, as you may well be aware.

Mr. Beatty: Sweden has that in there.

Mr. Hammond: Yes.

I am less troubled by the mechanics of doing the two things I suggested than perhaps some might consider I ought to be.

As far as unauthorized use is concerned, whatever it is called—and, clearly, there is a range of terminology that one could use there—my major concern is that it should be prefixed by the usual kind of criminal law safeguards and that it be without colour of right and this kind of thing, so that you do not run into the problem of the university student who runs over his time and this kind of thing. I have not seen any suggestion in any draft legislation anywhere that does not include these kinds of safeguards.

Likewise, I am not particularly disturbed when it comes to interference, whether it is called mischief or not. I do think you should be careful, though, as to what it is that the interference is with and that you should consider directing this to interference with data.

• 1700

Most communications theorists and I think most law draftsmen in this area draw a distinction between data and knowledge. In other words, if your top line is information, they say you have to break that down into two components: that

[Traduction]

gouvernement n'ont aucune raison de la protéger. Par exemple, il y a des compagnies qui font de la recherche sur le climat pour le gouvernement canadien. Le but de cette recherche est de fournir des renseignements aux universités et instituts de recherche afin qu'ils puissent l'utiliser et possiblement trouver de meilleures façons de prévoir le temps qu'il fera. À mon avis, toute disposition générale disant que toute donnée découlant des contrats gouvernementaux devrait être tenue secrète, serait très improductive. Je pense que plus de la moitié des renseignements sont transmis d'une façon ou d'une autre et de bon coeur. Par exemple, il y a diverses personnes qui sont à préparer des documents de travail sur des amendements à la Loi sur les brevets et à la Loi sur le droit d'auteur, ces personnes sont sous contrat avec le gouvernement canadien. Si on appliquait cette disposition générale, tous ces documents seraient secrets. En fait, j'essaie de mettre la main sur le plus grand nombre possible car je vais être en mesure de prévoir ce que le gouvernement fera.

M. Beatty: Merci, monsieur Fisk.

Professeur Hammond, vous avez suggéré la création de deux infractions, l'une pour l'usage non autorisée et l'autre pour «tripotage» des données, essentiellement.

Pour la première infraction, celle de l'usage non autorisée, une infraction semblable à celle de la violation de propriété, pour ce qui est des données, serait-elle appropriée? On pourrait parler de violation de l'ordinateur—essentiellement l'accès non autorisé?

M. Hammond: Comme vous le savez peut-être très bien, c'est là le genre de concept cohésif qui est populaire, surtout auprès de certains pays scandinaves.

M. Beatty: La Suède a une telle disposition.

M. Hammond: Oui.

Je suis moins préoccupé par les modalités d'application des deux suggestions que j'ai faites que je devrais peut-être l'être d'après certains.

Pour ce qui est de l'usage non autorisé, peu importe comment on l'appelle—et il est clair qu'il y a toute une terminologie que l'on pourrait utiliser—ma principale préoccupation c'est que cette infraction devrait être couverte par les protections et garanties habituelles du droit criminel et du droit apparent, et ainsi de suite, afin d'éviter le problème de l'étudiant d'université qui dépasse son temps et ainsi de suite. Dans tous les projets de loi que j'ai vus, on inclut ce genre de protections et de garanties.

Aussi, je ne suis pas particulièrement inquiet lorsqu'il s'agit d'immixtion, qu'on appelle cela un méfait ou autrement. Toutefois, je pense qu'il faut être prudent sur ce quoi porte cette immixtion et vous devriez envisager le problème relativement aux données.

Dans ce domaine, la plupart des théoriciens en communications et la plupart des rédacteurs de lois font une différence entre données et connaissances. Autrement dit, si votre principale préoccupation, c'est l'information, selon eux, vous

[Text]

data is something raw, that knowledge is another thing again. I think it is a useful technique to direct it to the data, not to the information itself.

Mr. Beatty: I think it goes to your second point, going back to unauthorized use, and your analogy of the chicken coop, which is a useful one. Presumably, if you can keep your neighbour from the door of the chicken coop you have solved the problem.

Mr. Hammond: You have gone a long distance.

Mr. Beatty: This is why it seems to me that something akin to data trespass, or unauthorized entry into the system—something along that line would probably at least close off the loophole that exists when you compare manually stored information to electronically stored information.

Mr. Hammond: I agree with that. My own impression with discussions within the industry is that they felt that would go some substantial distance towards meeting their concerns without creating the other kinds of problems that are raised at the second level.

Just in relation to that, I wondered if I could also clarify something in which I may have misled you in my opening. When I referred to draft legislation attached to my report, I was referring to a draft trade secrets protection act, not to draft criminal legislation. What that particular act would deal with—and I perhaps should put this on the table in case you have any questions about it for me while I am here—is that it involves three concepts. I agree entirely with Mr. Fisk's analysis of the present deficiencies with the law of breach of confidence. Essentially, it only applies if there is some trust-like relationship between discloser and discloser. The English royal commission, for instance, was very concerned in its report on breach of confidence, and I agree with its views, that it did not extend the law sufficiently far in the direction of what might be termed "industrial espionage".

What I have done in my draft legislation is to suggest that what is really needed is a new statutory tort—the word "tort" meaning a new civil wrong—which is composed of three key elements. Misappropriation By Improper Means of a Trade Secret: I have defined trade secret very widely—and it will become apparent why I refer to this—as including information, including a formula, patent, compilation, program, device, method, technique or process, that one derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and second, that is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. So if you do not keep your firm's equipment in proper order and you have not got a good security system, you do not get the benefit of the act.

[Translation]

devez la répartir en deux éléments: les données sont quelque chose de brut, alors que la connaissance est autre chose. Comme technique, je pense que c'est utile de considérer la question relativement aux données et non à l'information comme telle.

M. Beatty: Pour revenir à l'usage non autorisé, je pense que cela rejoint votre deuxième point et votre exemple du poulailler qui est un exemple utile. On suppose que vous réglerez le problème en éloignant votre voisin de la porte du poulailler.

M. Hammond: Vous avez fait un long chemin.

M. Beatty: C'est pourquoi il me semblait que quelque chose de similaire à la violation de propriété, pour ce qui est des données, ou à l'accès non autorisé au système, que quelque chose du genre pourrait au moins probablement combler la lacune qui existe dans l'emmagasinement électronique de l'information par rapport à l'emmagasinement manuel.

M. Hammond: Je suis d'accord là-dessus. Mon impression suite à des discussions avec des représentants de l'industrie, c'est que cela répondrait sensiblement à leurs préoccupations sans créer d'autres types de problèmes qui se posent au deuxième niveau.

A ce sujet, j'aimerais préciser quelque chose que j'ai dit dans mes remarques préliminaires et qui a pu vous induire en erreur. Lorsque j'ai fait allusion à un projet de loi annexé à mon rapport, je parlais d'un projet de loi sur la protection des secrets industriels et non d'un projet de loi criminel. Ce projet de loi, et je devrais peut-être le mettre sur la table au cas où vous me poseriez des questions à ce sujet pendant que je suis là, comporte trois concepts. Je suis complètement d'accord sur l'analyse de M. Fisk des lacunes actuelles de la loi pour ce qui est de l'abus de confiance. Essentiellement, cela s'applique uniquement s'il existe un genre de relation fiduciaire entre le divulgateur et la personne à qui ces divulgations sont faites. Par exemple, dans son rapport sur l'abus de confiance, la commission royale anglaise était très préoccupée du fait que la loi n'allait pas suffisamment loin dans ce que l'on peut appeler «l'espionnage industriel» et je suis d'accord avec son point de vue.

Dans mon projet de loi, j'ai suggéré que ce dont on avait vraiment besoin, c'était d'un nouveau préjudice statuaire... le mot «préjudice» signifiant une nouvelle injustice civile... composée de trois éléments clés. Détournement de secrets de fabrication par des moyens irréguliers: j'ai donné une définition très large au terme secrets de fabrication... et vous verrez pourquoi je fais allusion à ceci, pour inclure l'information, une formule, un brevet, une compilation, un programme, un dispositif, une méthode, une technique ou un processus, pouvant en soi représenter une valeur économique, existante ou possible, du fait de ne pas être généralement connue d'autres personnes pouvant tirer profit d'une telle divulgation ou utilisation, et qui ne peuvent vérifier à moins de disposer des moyens nécessaires, et, deuxièmement, qui font l'objet d'efforts raisonnables pour conserver ce secret, compte tenu des circonstances. Donc, si le matériel de votre entreprise n'est pas en bon état et si vous n'avez pas un bon système de sécurité, vous n'êtes pas protégés par loi.

[Texte]

Then as far as the misappropriation is concerned, that goes to acquisition, disclosure or use—including in some circumstances the man who gets the chicken sandwiches, although that is curtailed.

Under Improper Means; I have also included: "as a result of doing any of the following acts without authority, express or implied." And included in this is (c):

without prejudice to various other things, using or interfering with any computer or data retrieval mechanism, whether as regards any such act the absence of authority relates to his doing it at all, or only as to the manner or purpose in or for which he in fact does it.

Then the act provides a range of remedies that a court can apply. It also—and this is another matter that I perhaps should have mentioned in opening . . . it is a little confusing today to talk about the sharp distinction between criminal law and civil law. One of the things that I have done in this act is to make provision for exemplary or punitive damages: up to twice the amount of actual damages suffered can be awarded by the court in the civil suit. So you have an element of both taking away the gains of the wrongdoer, and also an element of punishment built into it.

• 1705

What has happened in the United States is that the definition of "trade secret," which I have suggested there, has also been adopted by a number of criminal codes. So that what has happened is that once you get this body of law into place, several legislatures there have simply adopted for criminal purposes the definition of a trade secret and also made it a criminal offence carrying, in many cases, quite substantial penalties. So my proposal is—and, as I say, I do not disagree with Mr. Fisk's analysis of the deficiencies of the present law—if a revised act of the kind that I am suggesting were to be enacted, it would go some greater distance towards meeting the kinds of concerns that arise. And it does not quite fit the sharp criminal law/ civil law dichotomy that many of us grew up on.

It also fits with my general thesis that what you should really be trying to encourage is the provision of a . . . somebody recently used the term "an umbrella concept"—that you have a number of spokes on the umbrella and that you provide a series of umbrella laws so that the industry can choose which laws it is going to use, the mode of protection it is going to use.

A company like IBM, for instance, when I worked for them, is well equipped to deal with the bureaucratic process. It has massive in-house staff, facilities and so forth. It can deal with the complexities of patent and copyright laws. Its headquarters are in the place where those kinds of things happen. Other companies may want to rely more on contractual protection, trade secret protection. You give that range of protection that leads to an umbrella kind of a concept.

[Traduction]

Ensuite pour ce qui est du détournement comme tel, cela comprend l'achat, la divulgation ou l'utilisation, dans certains cas, cela vise même la personne qui reçoit les sandwichs au poulet, quoique c'est limité.

Sous la rubrique moyens irréguliers, j'ai aussi inclus: «Après avoir posé l'un des gestes suivants sans autorisation expresse ou sous-entendue.» Et (c) est inclus dans ceci:

Sans préjudice à diverses autres choses, en utilisant tout ordinateur ou appareil d'extraction des données ou en interférant avec ces ordinateurs ou appareils, soit concernant un tel geste en l'absence d'une autorité quelconque de le faire, ou seulement quant à la manière dont il le fait ou le but dans lequel il le fait.

Ensuite, la loi prévoit toute une série de correctifs qu'un tribunal peut appliquer. Il y a aussi—et c'est une autre chose que j'aurais peut-être dû préciser dans ma déclaration préliminaire—de nos jours cela crée peut-être un peu de confusion lorsque l'on parle de la distinction nette qu'il y a entre le droit criminel et le droit civil. L'un des choses que je fais dans cette loi, c'est de prévoir une indemnisation exemplaire ou punitive par rapport aux dommages subis. Et dans le cas d'une poursuite civile, le tribunal peut accorder jusqu'au double du montant des dommages réels. On fait ainsi d'une pierre deux coups en éliminant l'avantage qu'il y a à commettre un méfait et en punissant celui qui l'a commis.

Aux États-Unis, la définition de «secret de fabrication» que j'ai suggérée, a aussi été adoptée dans plusieurs codes criminels. Alors ce qui s'est passé, c'est qu'une fois qu'on a ces mesures législatives en place, de nombreuses législatures ont simplement adopté la définition de secret de fabrication aux fins de leur code criminel, et en ont également fait une infraction criminelle comportant, dans bien des cas des peines assez sévères. Je le répète, je suis d'accord avec l'analyse de M. Fisk des lacunes de la loi actuelle, alors ce que je propose c'est que si une loi révisée du genre que je suggère était adoptée, ce serait un grand pas d'accompli pour répondre aux genres de préoccupations qui se posent. Et cela ne correspond pas exactement à la dichotomie nette droit criminel—droit civil, avec laquelle beaucoup d'entre nous ont grandi.

Cela correspond aussi à ma thèse générale qu'il faut vraiment essayer d'encourager l'adoption d'un . . . Récemment quelqu'un a utilisé le terme de «concept parapluie» . . . Le parapluie comporte plusieurs rayons et vous pouvez avoir une série de lois parapluies de sorte que l'industrie peut choisir celle qu'elle utilisera, le mode de protection qu'elle utilisera.

Par exemple, j'ai travaillé pour IBM, cette compagnie est très bien équipée pour s'occuper du processus bureaucratique. Elle dispose d'un personnel-maison important, d'installations et ainsi de suite. Elle est en mesure de se retrouver dans la complexité des lois sur les brevets et sur les droits d'auteur. Ces bureaux chefs sont situés à l'endroit où ce genre de choses passe. D'autres compagnies voudront se fier davantage à la protection contractuelle, à la protection qu'offre la loi sur les secrets de fabrication. Alors, si vous donnez cette gamme de protection, vous avez ce genre de concept parapluie.

[Text]

The Chairman: I am sorry, you have had all of your 20 minutes.

Mr. Beatty: Just one last one. I have come to the end of my list, in any case, except that I wanted to pick one other nit, but we will set that aside.

Was this, then, the description of what you meant about the other offence of meddling with data? You talked about an offence that could be dealt with in the Criminal Code; of meddling with data, in essence. Is that under criminal laws in the trade secrets provision?

Mr. Hammond: No. The mischief analogy, I think, is the closest to it—that you really are doing two things to the Criminal Code. You are making unauthorized access, as such, a matter of criminal law proscription with the traditional criminal law safeguards attached to that. And secondly, the mischief analogy that has already been referred to, so that you get at the meddling with the data as well.

Mr. Beatty: Thank you very much.

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman. I want to congratulate both our witnesses here today, Professor Hammond and Mr. Fisk, for a very fine presentation. As my colleague has said, I think you have both been more than helpful. I will restrict my questions as much as I can because I think you have covered many of the matters that I was intending to raise, in any event.

But in going over some of the material—and before I do that I wonder, Professor Hammond, if you could make available to us this report you referred to on quite a number of occasions, and also your draft legislation? It might be very helpful, too, if you have no objection to leaving it with the committee.

Mr. Hammond: I am not sure whether you were present when I started in on this but the position is, as I have indicated, that I am a civil servant who prepared a report for an organization in the west and an organization in the east. I have submitted it to both. It is in draft form; I am going back to Edmonton to make one or two detail changes.

The suggestion is that this will be done by next week; and I personally, of course, have no objection whatsoever to its being made available. But I think the formal process would be through the Justice department. Mr. Hill is present; he is in charge of the project and I would suggest the committee would go through him for that particular . . .

Mr. Robinson (Etobicoke—Lakeshore): I am sure that Mr. Hill will be only too happy to co-operate. He is nodding his head, yes, so I am sure that . . . But you have referred to it and I think it would be helpful to us to have the benefit of that.

Professor Hammond, you also indicated that in your view the federal and provincial law is quite deficient, and you indicated that the civil law and the criminal law, for that

[Translation]

Le président: Je m'excuse, mais vos 20 minutes sont écoulées.

M. Beatty: Juste une dernière question. De toute façon, j'ai épuisé ma liste de questions, sauf qu'il y a un autre point que je voulais soulever, mais nous le mettrons de côté.

Alors, était-ce là la description de ce que vous vouliez dire par l'autre infraction de tripotage des données? Vous avez parlé d'une infraction qui pourrait être incluse dans le Code criminel, et il s'agit essentiellement de tripotage des données. Est-ce que cela relève des dispositions du Code criminel sur les secrets de fabrication?

M. Hammond: Non. Non, je pense que ce qui s'en approche le plus c'est le méfait . . . en vertu du Code criminel, vous faites deux choses. Vous vous rendez coupables d'un accès non autorisé, comme tel, en vertu de la prescription de la loi criminelle avec les protections et garanties traditionnelles rattachées au droit criminel, à cet égard. Et deuxièmement, il y a l'analogie avec le méfait auquel on a déjà fait allusion, donc, de cette façon, vous rejoignez également le tripotage des données.

M. Beatty: Merci beaucoup.

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président. Je tiens à féliciter nos deux témoins d'aujourd'hui, le professeur Hammond et M. Fisk, de leur excellent exposé. Comme mon collègue l'a dit, je pense que tous les deux, vous avez été plus qu'utiles. Je limiterai mes questions dans la mesure du possible car je pense que vous avez couvert beaucoup de sujets que j'avais l'intention de soulever de toute façon.

Mais en regardant certains documents . . . mais avant, professeur Hammond, est-ce que vous pourriez fournir au Comité ce rapport auquel vous avez fait allusion à plusieurs occasions ainsi que votre projet de loi? Cela pourrait également nous être très utile, si vous n'avez pas d'objection de les remettre au Comité.

M. Hammond: J'ignore si vous étiez là au début, mais, je le répète, ma position c'est que je suis un fonctionnaire qui a préparé un rapport pour une organisation de l'ouest et pour une organisation de l'est. J'ai soumis le rapport aux deux sous forme d'ébauche. Je retourne à Edmonton pour y apporter un ou deux changements.

Ce qui a été suggéré c'est que ces documents soient déposés la semaine prochaine et, bien sûr, je n'ai aucune objection à ce que cela se fasse. Mais je pense que la procédure officielle serait de passer par le ministère de la Justice. M. Hill est présent, c'est lui le responsable du projet et je suggérerais au Comité de s'adresser à lui pour ce . . .

M. Robinson (Etobicoke—Lakeshore): Je suis convaincu que M. Hill se fera un plaisir de coopérer avec nous. Il fait signe que oui, donc je suis sûr que . . . Mais vous y avez fait allusion et je pense qu'il serait utile que nous en ayons un exemple.

Professeur Hammond, vous avez aussi dit que selon vous que la Loi, tant fédérale que provinciale, est très déficiente, et en fait, vous avez dit que cela s'applique également aux droits

[Texte]

matter, both are quite deficient. It seems to me you are alluding that there should be a consensus *ad idem* of people at the provincial and federal levels working together in the civil end, to start with, and maybe also as far as the criminal law is concerned, so that you cover both the criminal law and the statute law and also cover it from the provincial and the federal points of view. You keep nodding your head yes, but you have not said anything.

• 1710

Mr. Hammond: I accept the thrust of what you are saying without any reservation. The only question arising in my mind is the appropriate manner of achieving that kind of objective. There are various ways in which it could be done. It could be done by an informal collaborative mechanism; it could be done by a federal-provincial task force kind of thing; the uniformity mechanism in Canada could be used.

I frankly am not as well placed as a number of other advisers in Ottawa, who have had more experience of those kinds of exercises, to tell you which would be the best of those alternatives. I have simply said, as a matter of principle, I would think this committee would be doing the country a service if it would firmly grasp the nettle on the interference side on the Criminal Code and also just as firmly emphasize the importance of making some real progress, on a collaborative basis, on what I have called the second-stage matters.

Mr. Robinson (Etobicoke—Lakeshore): So you think, really, we should reach out to all the provinces and ask them if they have any contribution to make with regard to this matter.

Mr. Hammond: It is a very difficult matter. Perhaps I can put this to you as frankly as I can, again speaking as a civil servant. The provinces know this matter is important nationally. They know that in many areas they are dealing with federal statutes. They know the jurisdictional questions are quite complex. They know organizations like the Economic Council and many of the federal bodies are interested in these matters, as they ought to be, because we are told they represent the new lifeblood of the country. We know from the pronouncements that are being made in the House and many government studies that this is where it is at.

The provinces, therefore, tend to look for some kind of lead; and they certainly do not necessarily want to act on their own, so they keep a weather eye cocked always to what the federal government may be going to do or what it thinks should happen, notwithstanding that they may have the jurisdiction. You get a rather catch-22 situation, where both are watching each other because of the jurisdictional complications, although there is general agreement on what should be done, and there is some necessity to break that circle. I am not sure on...

Mr. Robinson (Etobicoke—Lakeshore): I think we are only too happy and prepared to co-operate with the provinces in any way possible, and I think that goes for all of us here. We

[Traduction]

civils et aux droits criminels. Il semble que vous faites allusion au fait qu'il devrait y avoir un consensus *ad idem* de gens au niveau des provinces du fédéral, travaillant ensemble sur le Code civil d'abord et peut-être aussi pour ce qui est du droit criminel, afin de couvrir le droit criminel et la jurisprudence du point de vue provincial et du point de vue fédéral. Vous hochez la tête en signe d'assentiment, mais vous n'avez rien dit.

M. Hammond: J'accepte sans réserve le sens de vos propos. La seule question qui me vient à l'esprit, c'est la façon appropriée d'atteindre ce genre d'objectif. Il y a diverses façons dont on peut le faire. Cela peut se faire par un mécanisme officiel de collaboration; cela peut se faire par un groupe de travail fédéral-provincial; on pourrait utiliser au Canada le mécanisme d'uniformité.

Franchement, je ne suis pas aussi en mesure de vous dire, comme le sont bon nombre d'autres conseillers d'Ottawa ayant plus d'expérience de ce genre d'exercices, laquelle de ces possibilités est la meilleure. J'ai simplement dit, comme question de principe, qu'à mon avis, le comité rendrait service aux clients s'il prenait le taureau par les cornes pour ce qui est de la question d'immixtion relativement au Code criminel et s'il mettait aussi fermement l'accent sur l'importance d'accomplir des progrès réels, sur une base de collaboration, sur ce que j'ai appelé les questions de deuxième niveau.

M. Robinson (Etobicoke—Lakeshore): Alors, vous pensez vraiment que nous devrions en toucher un mot à toutes les provinces afin de leur demander si elles peuvent apporter une contribution dans ce domaine.

M. Hammond: C'est une question très difficile. Je vais essayer de vous présenter la chose le plus franchement que je peux le faire, encore une fois à titre de fonctionnaire. Les provinces savent que c'est là une question d'importance nationale. Elles savent que dans bien des domaines, il s'agit de lois fédérales. Elles connaissent la complexité des questions de juridiction. Elles savent que des organismes comme le Conseil économique et bien d'autres organismes fédéraux sont intéressés par ces questions, comme ils doivent l'être, puisqu'on dit qu'elles représentent le sang nouveau du pays. Nous savons, d'après les déclarations faites en Chambre, d'après de nombreuses études gouvernementales que les choses en sont là.

Alors, les provinces ont tendance à rechercher un genre d'indice; elles ne veulent certainement pas agir de leur propre chef, alors elles veillent au grain sans perdre de vue ce que le fédéral peut faire ou ce que le fédéral pense qu'il devrait faire, en dépit du fait que cela relève de leurs compétences. Alors vous avez là un genre de cercle vicieux, où chaque partie surveille l'autre à cause des complications de compétence, quoiqu'on s'entende généralement sur ce qui devrait être fait. Il est donc nécessaire de briser ce cercle. Je ne suis pas sûr...

M. Robinson (Etobicoke—Lakeshore): Je pense que nous serions heureux de collaborer avec les provinces de quelque façon que ce soit et je pense que cela s'applique à tous ceux qui sont là. Nous comprenons l'importance de toute cette question

[Text]

realize the importance of this whole matter and we realize there is also a jurisdictional problem to be dealt with as well.

Let me get down to something else. You indicated that, in your view, getting a third of a loaf, half a loaf or a piece of the loaf or something was better than nothing. I think you were indicating there were a number of procedural steps that should properly be taken and that it could not be all done at once. I wonder if you can tell us what kind of priorities you would set. What is the first step? What is the second step? Is there a third step? Where do you go? What is the timeframe we are looking at to do this?

Mr. Hammond: I tend to feel it is realistic to aim at the kind of Criminal Code amendments... that is, the unauthorized user, the data meddling, for want of a better term—at this time. I would prefer to see concurrently with that, if it is possible, while that is being done in a formal legislative way with federal assistance, whatever form it takes, these civil law reforms being got on with. So you would then be in a position—admittedly, some months hence... to come back and review, if you like, what, if any, further role there might be for the criminal law.

So you are talking about a timeframe of trying to tidy up the Criminal Code side of it as part of the omnibus bill, encouraging this collaborative effort on the other matters concurrently with that; and then, probably in the course of a further criminal law exercise, you would pick up on the remaining matters.

Mr. Robinson (Etobicoke—Lakeshore): That answer indicates to me that it could be a year or two before anything is done. Do you not feel there is some urgency to take some first steps, small as they may be, with regard to this whole question of...

• 1715

Mr. Hammond: I clearly regard, from a personal point of view—I am not sure what the legislative timetable could be in realistic terms; I do not know what the situation is in this House—but I do regard the question of unauthorized user and data meddling as something that ought to be attended to as a matter of real urgency.

Mr. Robinson (Etobicoke—Lakeshore): You mentioned that you recommended, I guess, a review of restrictive covenants and contracts and also a review of the notion of unfair competition. I wonder how you relate this to the subject matter before the committee?

Mr. Hammond: That is why I did not dwell on it at length, because of course, both those matters fall within provincial jurisdiction. But they are quite important, and one can learn a lot from California in this respect.

California is the high tech state in the United States. California does not allow any restrictive covenant regarding the mobility of employment in high tech industries. That flies in the face of all the conventional wisdom, and one would think that the system would not function without it. And yet it does.

[Translation]

et nous comprenons qu'il y a aussi des problèmes de concédence qu'il faut également régler.

Je veux passer à autre chose. Vous avez dit que selon vous, un tiers, une demie ou une partie du gâteau valait mieux que rien du tout. Je pense que vous avez dit qu'il y avait un certain nombre de mesures procédurales qui devraient être prises et qu'on ne pouvait pas tout faire en même temps. Pourriez-vous nous dire le genre de priorités que vous fixeriez. Quelle serait la première étape? Quelle serait la deuxième? Y en a-t-il une troisième? Où vous dirigez-vous? Quelle est la période de temps envisagée pour accomplir tout cela?

M. Hammond: Pour l'instant, je pense qu'en pratique, on peut viser le genre d'amendements à apporter au Code criminel, c'est-à-dire en ce qui touche l'usage non autorisé, le tripotage des données, à défaut d'un meilleur terme. Je préférerais en même temps, si possible, pendant que cela se fait par des voies de mesures législatives officielles avec l'aide du fédéral, ou quelle que soit la forme, que l'on entreprenne aussi la réforme des lois civiles. Alors, vous seriez donc en mesure... plusieurs mois par après, bien sûr... de revenir et examiner, si vous voulez, le cas échéant, quel autre rôle pourrait jouer le droit criminel.

Donc, on parle d'un calendrier pour essayer d'amender l'aspect Code criminel dans le cadre d'un projet de loi omnibus, et, en même temps, en encourageant cet effort de collaboration sur d'autres sujets; ensuite, probablement dans le cours d'une longue révision du droit criminel, vous pourriez vous occuper du reste.

M. Robinson (Etobicoke—Lakeshore): D'après votre réponse, cela veut dire un an ou deux avant d'arriver à quoi que ce soit. Ne pensez-vous pas qu'il est urgent de prendre une première mesure, aussi minime soit-elle, au sujet de toute cette question de...

M. Hammond: D'un point de vue personnel, je considère certainement... n termes pratiques, j'ignore quel serait le calendrier législatif; j'ignore quelle est la situation de la Chambre... La question d'usage non autorisé et le tripotage des données sont des questions dont il faut s'occuper d'urgence.

M. Robinson (Etobicoke—Lakeshore): Vous avez aussi dit que vous recommandiez un examen des ententes des contrats restrictifs et aussi de la notion de concurrence injuste. Comment reliez-vous cela à la question étudiée par le Comité?

M. Hammond: C'est pourquoi je ne me suis pas étendu longtemps sur le sujet puisque, bien sûr, ces deux questions relèvent de la compétence des provinces. Mais ce sont là des questions très importantes et on peut apprendre beaucoup de l'expérience californienne dans ce domaine.

Aux États-Unis, la Californie est l'État de la haute technologie. La Californie ne permet aucune entente restrictive au chapitre de la mobilité de l'emploi dans les industries de technologie de pointe. Cela est contraire à toute la sagesse conventionnelle et l'on serait porté à croire que le système ne

[Texte]

Suggestions are also presently being made in California, again in the high tech industries, that what is really involved in a lot of these cases is employee theft. And some people are seriously suggesting that we ought to consider a criminal law offence which is somewhat under that umbrella of theft by an employee, which is a novel concept and one which has just come to my attention.

What I did want to do, simply by including them in my package of possibilities, was really to indicate this notion that there are a number of things that can be done at different levels of government and that all of these things do need to be addressed. It was really for the matter of completeness. That is not something that the federal government could do anything about unless you accepted—and I think it could be fairly described as a minority view—that there is some residual federal jurisdiction under the federal Trade Marks Act. There is a provision in the federal Trade Marks Act, which was held to be unconstitutional, going to unconscionable business conduct. The Supreme Court held that that was unconstitutional. I believe there are some federal lawyers who maintain that there may be some residual jurisdiction left there.

Mr. Robinson (Etobicoke—Lakeshore): You indicated, Professor Hammond, that you would not recommend a Criminal Code offence being imposed on the data processing industry for failure to take reasonable care. And yet your colleague, when he was talking about trade secrets, has a statement here that it is only applicable in cases where a person has a secret and takes all reasonable steps to keep it secret.

Now, I realize that you are speaking maybe in a very generic way, and your colleague, Mr. Fisk, was speaking about trade secrets per se. But is there not some consensus between you that...

Mr. Hammond: I think there is. I think that what we were saying was that in areas like security and certain selective areas, there are already various proscriptions. And indeed, one survey that we did of federal statutes showed that there are 51 federal statutes which have some provisions relating to confidentiality of information of one kind or another, and that will be available as part of the appendix.

What I was also emphasizing is that, in a general way, you do not get your civil law remedy unless you have taken satisfactory steps. You just cannot sue on it. So it is a negative kind of way of enforcing that obligation.

I think one of the first things you always have to do in a case of the kind that we are discussing, a misappropriation of information case... and even if you do not raise it the judge will—there will be a pretty firm inquiry as to what you did to look after this stuff. And if your own in-house measures are not suitable, you simply will not have a civil remedy. So indirectly you are forced to do so.

[Traduction]

fonctionnerait pas sans cela. Et pourtant il fonctionne. Présentement en Californie, encore une fois dans les industries de haute technologie, on croit que dans bien des cas, il s'agit de vols de la part d'employés. Et certaines personnes suggèrent sérieusement que nous devrions envisager une infraction de droit criminel qui soit en quelque sorte sous le concept parapluie de vol par un employé, ce qui est un concept nouveau et qui vient juste d'être porté à mon attention.

Ce que je voulais faire simplement en le mentionnant parmi les possibilités, c'était vraiment de vous faire voir qu'il est possible de faire plusieurs choses à différents paliers de gouvernement et qu'il faut s'occuper de toutes ces choses. C'était vraiment pour vous présenter un portrait complet. Le gouvernement fédéral ne peut rien y faire à moins que vous reconnaissiez... et je pense qu'on pourrait dire à juste titre qu'il s'agit là d'une opinion minoritaire... qu'en vertu de la Loi sur les marques de commerce il y a une compétence fédérale résiduelle. Il y a une disposition de la Loi fédérale sur les marques de commerce, touchant la conduite d'affaires inadmissible, qui fut jugée inconstitutionnelle. La Cour suprême a maintenu que cette disposition était inconstitutionnelle. Je pense que certains avocats fédéraux maintiennent qu'il y a là une compétence résiduelle.

M. Robinson (Etobicoke—Lakeshore): Professeur Hammond, vous avez dit que vous ne recommandez pas que l'on considère comme une infraction au Code criminel le fait qu'une industrie de traitement de données ne prenne pas de mesure raisonnable. Toutefois, votre collègue, alors qu'il parle des secrets de fabrication, mentionne dans sa déclaration que cela s'applique uniquement dans les cas où la personne qui a un secret a pris toutes les mesures raisonnables pour le protéger.

Maintenant, je comprends que vous parlez de façon très générale alors que votre collègue M. Fisk parlait du secret de la fabrication comme tel. Mais n'y a-t-il pas un genre de consensus entre vous à l'effet que...

M. Hammond: Je le pense. Je pense que ce que nous disions, c'est que dans des domaines comme celui de la sécurité et certains domaines sélectifs, il y a déjà diverses proscriptions. Et en fait, d'après un relevé que nous avons effectué il ressort qu'il y a 51 lois fédérales contenant certaines dispositions portant sur la confidentialité de l'information d'une façon ou d'une autre; et cela sera disponible comme partie de l'annexe.

Ce sur quoi j'insiste également, de façon générale, c'est qu'à moins d'avoir pris des mesures satisfaisantes, vous ne pouvez pas vous prévaloir du droit civil. Vous ne pouvez tout simplement pas entamer de poursuite. C'est donc une façon négative de faire respecter cette obligation.

Je pense que l'une des premières choses que vous devez toujours faire dans un cas du genre dont nous discutons, soit détournements d'information... et même si vous ne le faites pas le juge le fera... c'est qu'on s'enquerra de façon très attentive sur ce que vous avez fait pour protéger ces renseignements. Et si vos mesures internes sont tout simplement insatisfaisantes, vous n'aurez simplement aucun recours en droit civil. Indirectement, vous êtes donc obligé de le faire.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): You would not want to go so far as to see charges being laid against . . .

Mr. Hammond: No, I will tell you what I am really worried about. It is that if you put a Criminal Code offence in, saying that—putting this in its shortest form, that every data processor has got to look after the security of the information that is in his keeping—then you have real concerns about the kind of costs that it imposes on the industry. You are using what really should be the vehicle of last resort, and I am not aware of . . . I am satisfied that there is sufficient empirical evidence of misappropriation of information that you should do something of the variety we have already discussed. There really is not available empirical evidence that I think would stand up against the data processing industry that would presently justify . . .

• 1720

Mr. Robinson (Etobicoke—Lakeshore): Would it be fair to say that you are in agreement that there should be some standard of care taken?

Mr. Hammond: Yes, but with this qualification: I think it is going to have to be worked out over a period of time with an eye to the particular situations that you are addressing. I do not think you can reach it on a general level.

Mr. Robinson (Etobicoke—Lakeshore): You mentioned something about self-regulation by the industry itself. You did not go into detail on that. I would like to know, basically, what it is you are really referring to. What is it that you feel that the industry itself could be doing? Is "regulation" something like having a press council kind of thing, making it open to the public to know? Is it a code of ethics of some kind? What are you really talking about when you talk about self-regulation?

Mr. Hammond: Leaving any educational role or any code of ethics to one side for one moment, that is clearly one possibility. The other matters that I raised, based on some work that had been done at the Harvard Business School as to just how you might go about regulating this kind of industry, were these: I think I broke it down into three categories. You could have what is called system licensing and inspection. This would involve restricting the offering of such services until the system contained permanent safeguards of the type outlined and you could have periodic inspection of the system. Secondly, you could have a system of system certification, which might be either voluntary or carried out by a government body, and the certificate would operate as an advice to the consumer that the system meets minimum security requirements. Or, thirdly, you might want to go to something like the licensing of personnel. The operating personnel could be required to meet externally mandated professional requirements. It is rather like the professional licensing of the medical or legal profession.

I guess what I am really saying to you, sir, is that, given this range of alternatives that go all the way from the educational

[Translation]

M. Robinson (Etobicoke—Lakeshore): Vous ne voulez pas qu'on aille jusqu'à porter des accusations contre . . .

M. Hammond: Non, je vais vous dire ce qui m'inquiète vraiment. Si vous voulez en faire une infraction au Code criminel en disant que . . . Pour résumer, que chaque entreprise de traitement de données doit voir à la sécurité de l'information dont elle a soin . . . alors il y a un problème réel quant au genre de coûts que cela impose à l'industrie. Vous faites vraiment appel à ce qui devrait être un mécanisme de dernier recours, et à ma connaissance il n'y a pas . . . Je suis convaincu qu'il y a suffisamment de preuves empiriques de détournement d'informations que vous devriez faire quelque chose au sujet des types dont nous avons déjà discuté. Il n'y a vraiment pas de preuves empiriques disponibles qui puissent, à mon avis, être invoquées contre l'industrie de traitement de données, pouvant présentement justifier . . .

M. Robinson (Etobicoke—Lakeshore): Serait-il juste de dire que vous êtes d'accord qu'il faille établir des normes pour les mesures à prendre?

M. Hammond: Oui, mais avec cette précision: je pense qu'il faudrait que cela se fasse sur une certaine période de temps en tenant compte des cas particuliers auxquels cela s'applique. Je ne pense pas que cela peut se faire sur une base générale.

M. Robinson (Etobicoke—Lakeshore): Vous avez parlé d'auto-réglementation par l'industrie elle-même. Vous n'êtes pas entré dans les détails à ce sujet. En somme, j'aimerais savoir ce à quoi vous faites vraiment allusion. Selon vous, qu'est-ce que l'industrie elle-même pourrait faire? Est-ce que par "réglementation" vous entendez quelque chose comme un conseil de presse, quelque chose qui soit ouvert afin que le public s'en soit informé? S'agit-il d'un genre de code déontologique? De quoi parlez-vous vraiment, lorsque vous parlez d'auto-réglementation?

M. Hammond: Laissons de côté un instant le rôle éducatif toute question de code déontologique, c'est nettement là une possibilité. Voici les autres questions que j'ai soulevées sur la façon de réglementer ce genre d'industrie en me basant sur certains travaux effectués à la 'Harvard Business School' et je pense les avoir répartis en trois catégories. Vous pourriez avoir ce que l'on appelle l'inspection des systèmes et l'émission de permis. Cela signifie que l'on limite la fourniture de tels services jusqu'à ce que les systèmes contiennent des mesures de protection permanente du type de celles qu'on a mentionnées, et vous pourriez avoir des inspections périodiques du système. Deuxièmement, vous pourriez avoir qu'un système de certificats, soit sur une base volontaire ou effectué par un organisme gouvernemental, et ce certificat serait comme un avis aux consommateurs disant qu'un tel système répond aux exigences minimum de sécurité. Ou, troisièmement, vous voudrez peut-être envisager l'émission de permis au personnel. Le personnel devrait répondre à certaines exigences professionnelles fixées par un organisme externe. Cela ressemble un peu aux licences professionnelles accordées aux médecins et aux avocats.

En fait, ce que je veux dire, c'est que compte tenu de toutes ces possibilités allant à la solution éducative en passant par

[Texte]

solution through the ethical code solution, through these various kinds of regulatory solutions and on into the Criminal Code, I would urge you not to take the Criminal Code route until you had had a pretty thorough investigation of these other alternatives.

Mr. Robinson (Etobicoke—Lakeshore): You indicated, Professor Hammond, that you were not concerned about concurrent remedies at all and you did not explain exactly what you meant by concurrent remedies. Were you thinking in terms of federal statutes and provincial statutes, or were you thinking of a federal-provincial mix as against the Criminal Code provisions?

Mr. Hammond: When you set up a legal regime, you necessarily have to classify conduct into a series of slots into which you are going to put them. Some people who design legal systems and legal regimes will tell you that it is, for one reason or another, undesirable that more than one of these boxes could potentially apply to the particular conduct. When you press them about what is wrong with that, with the fact that a plaintiff should be able to choose between them if he wants to, the answer you will usually get comes down to some fairly technical things, like the time limit differs under each statute or the jurisdiction gets to be a problem, or the remedies differ. I guess my position is that I just do not find that as difficult in practice as some people have suggested and, indeed, I much prefer a legal solution that does provide a range of possible causes of action and leaves it to the individual adviser to make up his mind as to which of those best fits his client's case.

Mr. Robinson (Etobicoke—Lakeshore): I think you also talked about a new tort being created, but we have no law on it as yet, or very little. Do you think there will be a body of law built up on this in the immediate future?

Mr. Hammond: What I have done has been to take the existing common law body and extend it in the form of a statutory tort. It is always useful, to me at least, as somebody who used to practise law, to try to write it down in the form of a statute.

• 1725

I find it is a more definite kind of thing. You have to decide so many coverage questions which I think are important. What I am really suggesting with that is that it is a draft piece of legislation which could usefully be considered for possible adoption through one of these uniformity types of mechanism.

Mr. Robinson (Etobicoke—Lakeshore): Mr. Fisk, you spoke about paranoia somewhere here . . .

Mr. Fisk: That is correct. I used the term.

Mr. Robinson (Etobicoke—Lakeshore): So did your colleague, in effect. He was referring to it, too.

Mr. Fisk: I think it would be early in my material; I believe at the bottom of page 1 of my material.

[Traduction]

celle du code déontologique, jusqu'aux divers types de solutions réglementaires et même à celles du code criminel, c'est que je vous incite à ne pas choisir la voie du code criminel d'ici à ce que vous ayez examiné de très près ces autres possibilités.

M. Robinson (Etobicoke—Lakeshore): Professeur Hammond, vous avez dit que les remèdes concomitants ne vous inquiétaient pas du tout et vous n'avez pas expliqué ce que vous vouliez dire par remèdes concomitants. Pensez-vous aux lois fédérales et provinciales, ou à un mélange de mesures fédérales—provinciales par opposition aux dispositions du code criminel?

M. Hammond: Lorsque vous établissez un régime juridique, vous devez nécessairement catégoriser le comportement dans une série de créneaux où vous allez les classer. Certaines personnes qui conçoivent les systèmes et régimes juridiques vous diront, que pour une raison ou pour une autre, il n'est pas souhaitable que plusieurs de ces créneaux puissent possiblement s'appliquer à un comportement en particulier. Lorsque vous insistez pour savoir ce qu'il y a de mal à ça, ce qu'il y a de mal au fait que l'accusé devrait pouvoir choisir entre ces créneaux s'il le désire, la réponse porte habituellement sur des aspects très techniques, à savoir que la limite de temps varie selon chaque loi ou qu'il y a des problèmes de compétence, ou que les correctifs sont différents. Ma position c'est qu'en pratique je ne pense pas que ça pose autant de difficultés que certaines personnes l'ont suggéré et je préfère de loin une solution juridique qui offre plusieurs possibilités d'action et laisse le soin à l'avocat de déterminer lequel convient le mieux à son client.

M. Robinson (Etobicoke—Lakeshore): Je pense que vous avez également mentionné qu'on avait un nouveau préjudice sur lequel nous n'avons aucune loi jusqu'à présent ou très peu. Croyez-vous qu'il y aura un ensemble de lois sur cette question dans un avenir immédiat?

M. Hammond: Ce que j'ai fait j'ai pris les lois existant dans la common law et je les ai élargies sous forme de préjudices statutaires. C'est toujours utile, du moins pour moi qui ai déjà pratiqué la loi, d'essayer de rédiger une chose sous forme de statut.

Je pense que c'est une chose beaucoup plus claire. Vous devez décider de tellement de questions d'application ce qui, je pense, est important. Ce que je prétends en réalité c'est qu'il s'agit là d'un projet de loi qui pourrait utilement être considéré pour adoption par le truchement d'un de ces mécanismes de type uniforme.

M. Robinson (Etobicoke—Lakeshore): Monsieur Fisk, dans ce document vous faites allusion à la paranoïa.

M. Fisk: En effet. J'ai utilisé ce mot.

M. Robinson (Etobicoke—Lakeshore): Votre collègue y a également fait allusion.

M. Fisk: Je pense que ce serait au début de mon document, au bas de la page 1.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): To my mind it means you feel the companies in the field of computer software—by being paranoid, they feel as though they are being persecuted in some way. I do not really understand your analogy. To me, they would be more inclined to be schizophrenic.

Mr. Fisk: No...

Mr. Robinson (Etobicoke—Lakeshore): Let me complete this. In other words, in my view they may not be really in touch with the reality of the situation; and they should be, because they are in the business. They should know this problem, and they should know it well. They should not only perceive it, but they should be doing something about it. I think it is all very well to talk about the Dr. Moriarity—you both mentioned him—as always taking on challenges for the sake of taking on a challenge or trying to do something that is impossible just to be able to say, well, “impossible” merely means that it is difficult to do. That is what they are doing with this computer set-up.

But by the same token, you need a Sherlock Holmes. I have never heard Dr. Moriarity's name used when you did not at the same time use Sherlock Holmes. That is the counterpart or the countervailing weight. Where do you see the Sherlock Holmes coming into this situation?

Mr. Fisk: At the moment the situation with a company is it has to employ highly trained programmers. These programmers, of course, are likely at any time to go to another company if they get a better offer. When they go to the other company, many of them may take with them all this software which was laboriously put together. So companies are very afraid that their software is going to vanish out the door. If it does not vanish out the door in that way, it may vanish out the door by, let us say, somebody looking through their garbage bags or something of this sort. There are many ways that software can be stolen—or somebody with an antenna directed at their office to pick up electromagnetic pulses.

So companies live in an atmosphere of fear. They have put all this money into creating software. They have put years of development into it; and they realize a minute, one minute, of inattention and that can go out. So you find in many companies a great deal of fear.

I used “paranoia” because this is really a condition of extreme fear, sometimes where the most common things are perceived as threats. And companies do act that way, because one of those common things just might be a threat.

Mr. Robinson (Etobicoke—Lakeshore): I would love to go into some questions on that, but I am afraid I am restricted to one question, so I am going to ask you this. You mention certain protection laws that we have now—namely in trade secrets, trade marks, copyright and patent law—and that they would need amending. Have you considered the kind of amendments that might cover the computer industry? Along with that, since I only have this one question, I wanted to

[Translation]

M. Robinson (Etobicoke—Lakeshore): Si j'ai bien compris, selon vous, les compagnies oeuvrant dans le domaine du logiciel d'ordinateur, en étant paranoïaques, se sentent persécutées d'une façon ou d'une autre. Je ne comprends vraiment pas votre analogie. Je les penserais plus portées à la schizophrénie.

M. Fisk: Non.

M. Robinson (Etobicoke—Lakeshore): Laissez-moi terminer. Autrement dit, selon moi elles ne sont peut-être pas vraiment en contact avec la réalité de la situation et elles devraient l'être puisqu'elles oeuvrent dans le domaine. Elles devraient être au courant de ce problème et devraient bien le connaître. Elles devraient non seulement le percevoir, mais elles devraient prendre des mesures à cet égard. Je pense que c'est très bien de parler du Dr Moriarity, vous y avez tous deux fait allusion, comme quelqu'un qui relève toujours le défi pour le simple plaisir de la chose ou qui essaie de faire une chose impossible simplement pour pouvoir dire qu'impossible signifie simplement une chose difficile à accomplir. C'est ce qu'ils font avec ces ordinateurs.

Mais vous avez aussi besoin d'un *Sherlock Holmes*. Chaque fois que je vous ai entendu mentionner le nom du Dr Moriarity, vous avez aussi mentionné celui de *Sherlock Holmes*. C'est la contrepartie ou le contrepoids. Où voyez-vous l'intervention de *Sherlock Holmes* dans ce cas?

M. Fisk: La situation actuelle d'une compagnie, c'est qu'elle doit employer des programmeurs très qualifiés. Bien sûr, ceux-ci peuvent très bien passer à une autre compagnie s'ils reçoivent une meilleure offre. Lorsque cela arrive, beaucoup d'entre eux emportent avec eux ce logiciel qui fut laborieusement conçu. Donc les compagnies qui craignent énormément que leur logiciel disparaisse avec l'employé. Si cela ne se produit pas de cette façon, cela peut arriver alors que quelqu'un fouille dans leurs sacs à poubelle ou quelque chose du genre. Il y a plusieurs façons de voler le logiciel... ou quelqu'un peut capter les pulsations électromagnétiques à l'aide d'une antenne orientée vers leur bureau.

Donc les compagnies vivent dans une atmosphère de crainte. Elles ont investi tout cet argent pour créer ce logiciel. Elles y ont consacré des années d'efforts et de développement et elles s'aperçoivent qu'il suffit d'une minute d'inattention pour que tout cela disparaisse. Alors vous constatez qu'il y a une très grande crainte chez beaucoup de compagnies.

J'ai parlé de «paranoïa» car c'est vraiment là la condition de la peur extrême, alors que les choses les plus anodines peuvent être perçues comme des menaces. Et les compagnies se comportent de cette façon car l'une de ces choses les plus anodines peuvent être tout simplement une menace.

M. Robinson (Etobicoke—Lakeshore): J'aimerais beaucoup vous questionner là-dessus, mais je crains que je suis limité à une seule autre question, alors voici ce que je veux vous demander. Vous avez parlé de certaines lois de protection que nous avons présentement... c'est-à-dire sur les secrets de fabrication, les marques de commerce, les droits d'auteur et les brevets... et vous avez dit qu'elles auraient besoin d'être amendées. Avez-vous étudié le genre d'amendements qui

[Texte]

bootleg this in: Have you been looking at the Income Tax Act when you decided the kind of penalties or damages that should be meted out, to the extent that you are talking about twice the damages?

Mr. Fisk: It was Professor Hammond who talked about twice the damages.

Mr. Robinson (Etobicoke—Lakeshore): I am trying to bootleg that in.

Mr. Fisk: First, as to the type of amendments, I did give you some fairly concrete suggestions in my material on the Copyright Act.

• 1730

As for the Patent Act, I am not sure that specific amendments are needed except to deal with the question of the degree of unobviousness that is required. I am concerned that if a low standard of unobviousness is required there will be a lot of patents on marginal inventions, which might then impede the industry. If there is a reasonably high standard of unobviousness required, then I think the Patent Act as it currently stands would be all right.

As regards trade secrets, that is currently judge-made law and judges have a great deal of power to amend it as they see fit. Professor Hammond has suggested that one way of dealing with the inadequacies of trade secrets is by putting in a statute as well. I had not heard that before today. My immediate reaction to it is I see nothing wrong with it. I would like to see the statute before committing myself further, of course, because, to get agricultural again, you do not want to buy a pig in a poke.

Just one comment on trade secrets. Professor Hammond has referred to the problem that arose with respect to Section 7(e) of the Trade Marks Act. Now, that was federal legislation. It was held unconstitutional in the case of *Vapor Corporation v. McDonald*. It was held unconstitutional on the basis that it was not a regulatory statute. It would appear that in the area of trade secrets and unfair competition the federal government would have power if the statute were regulatory but it does not have power to set up a standard of conduct as between two individuals. It may well be, then, that if the provinces cannot be coerced or persuaded into bringing forth their own statutes, as Professor Hammond had suggested, one other possibility would be to set up some sort of a regulatory statute by which, for example, just as copyrights are now registered, trade secrets could be registered and that might accomplish the same thing. As I say, though, today is the first time I have heard of this so this is just an immediate, off-the-cuff reaction.

The Chairman: I would like to thank our two witnesses of this afternoon. I am quite sure we could continue for a couple more hours. We hope to be able to share the results of your study in the near future when it is completed.

[Traduction]

pourraient couvrir l'industrie de l'ordinateur? Puisque je n'ai qu'une seule question, je voudrais y raccrocher ceci: avez-vous envisagé la Loi de l'impôt sur le revenu lorsque vous avez décidé du genre de peine ou de dommage qui devrait être imposé, dans la mesure où vous parlez d'accorder des dommages doubles?

M. Fisk: C'est le professeur Hammond qui a mentionné cela.

M. Robinson (Etobicoke—Lakeshore): J'essaie de passer cette question en douce.

M. Fisk: D'abord, pour ce qui est du genre d'amendement, je vous ai fait des suggestions assez concrètes dans mon document sur la Loi sur le droit d'auteur.

Quant à la Loi sur les brevets, je ne suis pas persuadé qu'il faille y apporter des modifications précises sauf pour y aborder la question du manque d'évidence et qui pourrait se faire jour. Je crains que s'il faut y introduire un faible degré de manque d'évidence, de nombreux brevets portant sur des inventions marginales pourraient être déposés contrecarrant ainsi les projets de ce secteur industriel. S'il faut y introduire un degré relativement élevé de manque d'évidence, je pense alors que la Loi sur les brevets, sous sa forme actuelle, se suffit à elle-même.

En ce qui concerne le secret entourant les marques de commerce, cela relève de la compétence des juges qui ont tout le loisir de modifier cette loi s'ils le jugent nécessaire. Le professeur Hammond a proposé que l'on pourrait combler les lacunes inhérentes aux marques de commerce en adoptant une loi également. Je n'avais jamais entendu cela auparavant. De prime abord, je n'y vois pas d'inconvénient. Cependant, je voudrais voir la loi avant de m'engager plus en avant car cela reviendrait à acheter quelque chose les yeux fermés.

Une dernière observation sur les secrets industriels. Le professeur Hammond a fait allusion au problème survenu aux termes de l'alinéa 7^e) de la Loi sur les marques de commerce. Il s'agissait d'un texte de loi fédérale qui a été déclaré inconstitutionnel dans l'affaire *Vapor Corporation v. McDonald*, et ce, car il ne s'agissait pas d'une loi portant réglementation. Dans le domaine des secrets industriels et de la concurrence déloyale, il semblerait que le gouvernement fédéral détiendrait un certain pouvoir si la loi portait réglementation, mais il n'a aucun pouvoir lorsqu'il s'agit d'établir une norme de conduite entre deux individus. Dans ce cas, si les provinces ne peuvent pas être amenées à adopter leurs propres lois, comme le professeur Hammond l'a suggéré, un autre moyen serait d'établir une espèce de loi portant réglementation qui permettrait de déposer des secrets industriels tout comme les droits d'auteur le sont. Je le répète, c'est la première fois aujourd'hui que j'entends parler de tout cela et il s'agit donc de commentaires qui me viennent immédiatement à l'esprit.

Le président: Je voudrais remercier nos deux témoins de cet après-midi. Je suis sûr que nous pourrions continuer pendant au moins deux heures de plus et j'espère que nous pourrions discuter des résultats de votre étude lorsqu'elle sera terminée.

[Text]

I would like to invite members of the subcommittee to reconvene tomorrow at 9.30 a.m. with representatives of the Canadian Association of Data Processing Services, and thank you for joining us this afternoon.

The meeting is adjourned.

[Translation]

Je voudrais inviter les membres du sous-comité à reprendre leurs travaux demain à 9h30, heure à laquelle nous entendrons les représentants de l'Association canadienne des entreprises de services en informatique. Je vous remercie d'être venus cet après-midi.

La séance est levée.



*If undelivered, return COVER ONLY to
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada K1A 0S9*

*En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada K1A 0S9*

WITNESSES—TÉMOINS

Professor Grant Hammond, Counsel, Law Center, University
of Alberta, Edmonton, Alberta;

Mr. George E. Fisk, Barrister, Gowling and Henderson,
Ottawa, Ontario.

Professeur Grant Hammond, avocat, Centre d'études juridi-
ques, Université d'Alberta, Edmonton, Alberta;

Me George E. Fisk, avocat, «Gowling and Henderson»,
Ottawa, Ontario.

HOUSE OF COMMONS

Issue No. 10

Thursday, May 19, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 10

Le jeudi 19 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

INCLUDING:

The Second Report to the Standing Committee on
Justice and Legal Affairs

CONCERNANT:

Questions relatives à l'ordre de renvoi

Y COMPRIS:

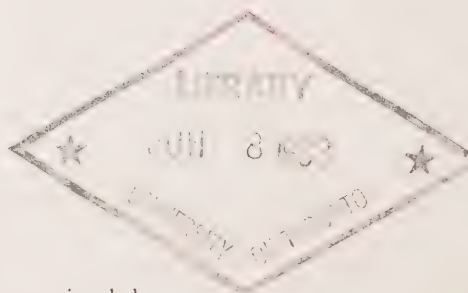
Le deuxième rapport du Comité permanent de la justice
et des questions juridiques

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trrente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

**RAPPORT AU COMITÉ PERMANENT DE LA JUSTICE
ET DES QUESTIONS JURIDIQUES****LE JEUDI 19 MAI 1983**

Le Sous-comité sur les infractions relatives aux ordinateurs
a l'honneur de présenter son

DEUXIÈME RAPPORT

Conformément à son ordre de renvoi du mardi 1^{er} mars 1983, concernant l'étude de l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions au droit de propriété relatifs aux ordinateurs, votre Sous-comité demande la permission pour qu'il soit habilité à retenir les services d'experts et aussi à employer le personnel professionnel et de soutien nécessaire, afin de poursuivre l'étude de son ordre de renvoi.

**REPORT TO THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS****THURSDAY, MAY 19, 1983**

The Sub-committee on computer crime has the honour to
present its

SECOND REPORT

In accordance with its Order of Reference of Tuesday, March 1st, 1983, respecting the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, your Sub-committee requests leave to be empowered to retain services of experts, and professional, technical and clerical staff as may be deemed necessary for the continuation of the consideration of its Order of Reference.

PROCÈS-VERBAL

LE JEUDI 19 MAI 1983
(12)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 9h44, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Céline Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: M. Paul C. Boire Sr., président de l'Association canadienne des entreprises de services en informatique (CADAPSO), Ottawa et M. D.W. Kay, gérant de district, Datacrown Inc., Ottawa.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations.

M. Robinson (*Etobicoke—Lakeshore*) assume la présidence.

Les témoins répondent aux questions.

A 10h44, la séance est suspendue.

A 10h46, la séance reprend.

L'interrogation des témoins se poursuit.

A 10h59, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

MINUTES OF PROCEEDINGS

THURSDAY, MAY 19, 1983
(12)

[Text]

The Sub-committee on computer crime met this day at 9:44 o'clock a.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Céline Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: Mr. Paul C. Boire Sr., president of the Canadian Association of Data Processing Service Organizations (CADAPSO), Ottawa and Mr. D.W. Kay, District Manager, Datacrown Inc., Ottawa.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements.

Mr. Robinson (*Etobicoke—Lakeshore*) assumed the Chair.

The witnesses answered questions.

At 10:44 o'clock a.m., the sitting was suspended.

At 10:46 o'clock a.m., the sitting resumed.

Questioning of witnesses resumed.

At 10:59 o'clock a.m., the Sub-committee adjourned to the call of the Chair.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Thursday, May 19, 1983

• 0943

Le président: La séance du Sous-comité sur les infractions relatives aux ordinateurs est maintenant ouverte.

Ce matin, nous recevons l'Association canadienne des entreprises de services en informatique (CADAPSO) qui est représentée par M. Paul C. Boire. M. D. W. Kay comparait également ce matin au nom de l'Association.

Bienvenue, monsieur Boire. Je vous cède la parole immédiatement.

M. Paul C. Boire (président, Association canadienne des entreprises de services en informatique (CADAPSO)): Merci, madame le président.

My name is Paul Bois, I am the president of CADAPSO, the Canadian Association of Data and Professional Services Organizations. With me is Wayne Kay, who is the Ottawa manager of Data Crown, one of the largest computer services companies in Canada, and a long-time member of CADAPSO.

Madam Chairman and members of this committee CADAPSO appreciates the opportunity to appear before you today to present our industry's position on this important issue.

• 0945

I noticed that in earlier testimony before this subcommittee, Superintendent Allen of the RCMP said that police statistics do not support the suggestion that there is a serious problem with the use of computers in criminal activities, and he made reference to the *Time* magazine issue of January 3. In that issue, Donn Parker has been quoted by a number of people—a specialist in computer abuse at SRI International, formerly the Stanford Research Institute—he is quoted there in *Time* as saying that nobody seems to know exactly what computer crime is, how much of it there is, and whether it is increasing or decreasing. But we do know that computers are changing the nature of business crime significantly.

I have contacted all of our members on this subject and, to be frank with you, not too many of them see computer crime as a critical issue right now. I hope that our comments and suggestions will be helpful to you in your work. And in relation to the fact that not too many of our members get excited about this at the present time, if I can mix a metaphor in relation to the Criminal Code, I think we would like to see the stable door closed before the horse gets out.

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le jeudi 19 mai 1983

The Chairman: This meeting of the Subcommittee on Computer Crime is now open.

This morning we are welcoming the Canadian Association of Data Processing Service Organizations (CADAPSO) in the person of Mr. Paul C. Boire. Mr. D.W. Kay is also representing the association this morning.

Welcome, Mr. Boire. You now have the floor.

Mr. Paul C. Boire (President of the Canadian Association of Data Processing Service Organization (CADAPSO)): Thank you, Madam Chairman.

Je m'appelle Paul Bois, je suis président de CADAPSO, l'Association canadienne des entreprises de services en informatique. Je suis accompagné de Wayne Kay, le gérant pour la région d'Ottawa de Data Crown, une des compagnies d'informatique les plus importantes au Canada, membre depuis très longtemps de CADAPSO.

Madame le président, messieurs les membres du comité, CADAPSO apprécie cette occasion de comparaître aujourd'hui pour présenter la position de l'industrie face à cet important problème.

J'ai vu dans un autre témoignage que vous avez entendu au comité que le surintendant Allen, de la GRC, vous a déclaré que les statistiques de la police auraient tendance à prouver que le problèmes des infractions relatives aux ordinateurs n'est pas très grave. Par la même occasion, il parlait d'un article paru dans le magazine *Time*, le 3 janvier. Dans ce numéro, Donn Parker est cité par un certain nombre de personnes—c'est un spécialiste en infractions relatives aux ordinateurs, pour le compte de SRI International, précédemment le *Stanford Research Institute*—bref, d'après le *Time*, il aurait déclaré que personne ne semble bien savoir ce qui constitue une infraction relative aux ordinateurs, dans quelle mesure c'est un phénomène courant, si cela augmente, ou si cela diminue. Ce que nous savons, toutefois, c'est que les ordinateurs ont une influence déterminante sur la nature des crimes commerciaux.

J'ai demandé à tous nos membres quelle était leur opinion à ce sujet et, pour être franc, je dois vous dire que rares sont ceux qui voient dans les infractions relatives aux ordinateurs un problème très grave. J'espère que nos observations et nos suggestions vous seront utiles. Quant au fait que ce sujet n'inquiète pas terriblement nos membres à l'heure actuelle, vous me permettrez de hasarder une métaphore à propos du Code criminel: ce serait tout de même une bonne chose de fermer les portes de l'écurie avant que les chevaux ne se sauvent.

[Text]

CADAPSO is an acronym for the Canadian Association of Data and Professional Service Organizations, and our office is here in Ottawa on Albert Street. We are the national association that represents corporate management in the computer services industry. There are a number of other computer organizations; they tend to represent more the working level people or practitioners. Our association represents the owners and managers of computer services and professional services and software companies. We have 70 companies ranging from the largest ones, who do over \$100 million of business a year, down to the smallest one-man companies and consultants, who do less than \$100 thousand in a year. We have data centres, professional services, custom software houses, contract programming firms, facilities management companies, suppliers of turnkey, mini, and micro computer systems, and a variety of other organizations that supply and service the industry. Our member companies cover just about all aspects of computer services.

We have been, as an association, around for 13 years, and we participate in international congresses to promote the progressive image of our association and our member companies. We are associated with the ADAPSO, which is the data processing association in the United States, with ECSA, which is the European Computer Services Association, and with JSIA/JIPCA, which is the Japanese Software Industries Association.

We have helped to organize and have participated in three world congresses to date. The first one was in Barcelona, Spain, in 1978. The second one was in the United States, in San Francisco, in 1980. And the third one was in Copenhagen, last April, in 1982. The fourth one will take place in 1984, in Tokyo. And our association, CADAPSO, will host the fifth, in Toronto, in 1986.

I would like to say a little bit about CADAPSO's objectives. We have published these in a little pamphlet that we put out for our members and prospective members. They are: to have a clearly visible presence at all levels of the media and the public; to promote the industry; to provide valid input to government decisionmaking—and we hope that our input today will be helpful to you, to this subcommittee; we try to provide group and individual services to our members to improve management methods and service possibilities; to develop an appreciation of high ethical and performance standards; and the creation of an atmosphere of general public acceptance for the data processing business.

• 0950

I noted, in reviewing the previous testimony before your subcommittee, that Mr. Robinson asked the question: should there not be a body set up of people in the computer industry

[Translation]

CADAPSO, c'est le sigle pour l'Association canadienne des entreprises de services en informatique, et notre bureau se trouve ici même, à Ottawa, rue Albert. Nous sommes une association nationale qui représente les directions des industries de services en informatique. Un certain nombre d'autres organisations liées aux ordinateurs existent qui représentent plutôt les travailleurs et les professionnels. Notre association, pour sa part, représente les propriétaires et les administrateurs dans le domaine des services en informatique, des services professionnels et des compagnies qui fabriquent du logiciel. Nous représentons 70 compagnies, les plus grandes, dont le chiffre d'affaires dépasse 100 millions de dollars par année, les plus petites, parfois des compagnies constituées d'une seule personne et d'experts, dont le chiffre d'affaires peut être inférieur à \$100,000 par année. Nous avons des centres de données, des services professionnels, des fabricants de logiciel personnalisé, des entreprises de programmation à contrats, des compagnies d'administration des installations, des fournisseurs de produits finis, de petits ordinateurs et de micro-ordinateurs. Nous représentons également toute une série de fournisseurs pour l'industrie et de compagnies de services. Nos compagnies membres regroupent pratiquement tous les aspects des services d'ordinateur.

Notre association existe depuis 13 ans, et nous participons aux congrès internationaux pour affirmer notre réputation progressiste et celle de nos compagnies membres. Nous sommes associés à l'organisme ADAPSO, l'association américaine de traitement des données, avec ECSA, l'association européenne de services d'informatique, ainsi qu'avec JSIA/JIPCA, l'association japonaise des industries de logiciel.

Jusqu'ici, nous avons participé à l'organisation de trois congrès mondiaux. Le premier, à Barcelone, Espagne, en 1978. Le deuxième, aux États-Unis, à San Francisco, en 1980. Le troisième, enfin, à Copenhague, en avril dernier, en 1982. Le quatrième aura lieu en 1984, à Tokyo. Enfin, notre association, CADAPSO, sera l'hôte du cinquième congrès, qui se tiendra à Toronto en 1986.

Maintenant, je veux vous parler des objectifs de CADAPSO. Nous les avons publiés dans un petit dépliant que nous distribuons à nos membres et à nos futurs membres. Les voici: une présence clairement établie dans tous les secteurs publics et dans les médias; une participation active aux décisions prises par le gouvernement, soit dit en passant, nous espérons que notre participation d'aujourd'hui vous sera utile, utile à ce sous-comité, nous essayons d'offrir des services collectifs et individuels à nos membres, pour leur permettre d'améliorer leurs méthodes administratives et leurs possibilités de service; de convaincre nos membres de la nécessité d'adopter des normes morales et des normes de travail élevées; enfin, de sensibiliser l'ensemble du public au secteur du traitement des données.

J'ai lu les comptes rendus d'autres séances de votre Sous-comité et j'y ai vu, entre autres choses, une question de M. Robinson: est-ce qu'il ne conviendrait pas de créer un orga-

[Texte]

who would monitor the industry, be responsible for it, set up codes of ethics and so on? Is this being done? Is it being contemplated?

The answer is that CADAPSO is that body. Thirteen years ago, CADAPSO was formed to accept that responsibility. And I would like to quote from our membership application, which contains a code of ethics right on the front page. It says:

A member firm shall comply with the by-laws, rules and regulations of the association as they may be from time to time and with any order or resolution of the officers of the association under the by-laws.

And there is a heading called "Standards of Conduct Affecting the Public Interest":

A member firm shall conduct its business at all times in a manner which will maintain the good reputation of the industry and its ability to serve the public interest. A member firm shall perform its professional services with integrity and due care. A member firm has a duty of confidence in respect of the affairs of any client and shall not disclose, without proper cause, any information obtained in the course of its services nor shall it in any way exploit such information to its advantage. A member firm shall not adopt any method of obtaining or attracting clients which tends to bring disrepute on the industry.

There is another section which deals with "Relations with Members and Non-Members Engaged in the Provision of Data Processing Services":

A member firm shall act in relation to any other member firm with the consideration due between professionals and which in turn it would wish to be accorded by the other member. A member firm shall not, in any advertising, discredit or attempt to diminish in any way the services of other members.

One of the things, I think, that has come out in testimony before this subcommittee is whether and to what extent the industry took steps to protect itself. And I would like to quote to you from some of the typical computer services contracts and software licences that are used by our member companies.

Definitions are critical in understanding and interpreting any contract and this is particularly true in our industry, where technical terms and concepts are used. Probably many of these technical terms are not readily understood even by the contracting end user or by a court. In most software licences, the word "program" is used rather than "product," in order to avoid any implication of tangibility. For the same reason, materials such as tapes or discs, which are tangible, are usually separated from the program. The word "materials" is usually used instead of "documentation." "Documentation" is a word that is commonly used in the industry, but "materials" is usually used in contracts in order to broaden the coverage and to avoid a possibly narrower technical definition of the term "documentation." Another word that appears in the industry frequently is the term "enhancement." This includes modifications, upgrades, improvements and other synonyms in current usage.

[Traduction]

nisme de gens de l'industrie informatique qui serait chargé d'une surveillance de l'industrie, de la mise en place de codes d'éthique, et cetera? Cela est-il fait? Envisage-t-on de le faire?

Je peux vous répondre que CADAPSO joue précisément ce rôle. Il y a 13 ans, CADAPSO a été créée dans le but même d'assumer cette responsabilité. Cela dit, je vais vous citer un passage de notre demande d'inscription qui contient, dès la première page, une sorte de code moral:

Une compagnie membre se conforme aux directives et à la réglementation en cours de l'Association ainsi qu'à toute résolution des responsables de l'Association en vertu des règlements.

Vient ensuite un titre: «Normes de comportement dans l'intérêt public»:

Une compagnie membre se comporte toujours de façon à assurer la bonne réputation de l'industrie et son dévouement à l'intérêt public. Une compagnie membre s'acquitte de ses services professionnels avec intégrité et exactitude. Une compagnie membre respecte le caractère confidentiel des affaires de ses clients et ne révèle pas, sans bonne raison, les informations recueillies en cours de service; en aucun cas elle n'exploite ces informations pour en tirer un avantage. Une compagnie membre ne cherche pas à attirer des clients par des moyens qui pourraient donner une mauvaise réputation à l'industrie.

Il y a un autre passage qui parle des «relations avec les membres et les non-membres assurant des services de traitement des données»:

Une compagnie membre se comporte envers toutes les autres compagnies membres avec la considération qui s'impose entre des professionnels, et vice versa. Une compagnie membre ne cherche jamais, par publicité, à discréditer ou à diminuer d'une façon quelconque les services des autres membres.

Pendant vos délibérations, je sais qu'un sujet est apparu: dans quelle mesure l'industrie prend des mesures pour se protéger elle-même. À ce sujet, je veux vous citer un contrat typique utilisé par nos compagnies membres pour les services d'ordinateurs et les licences de logiciel.

Pour bien interpréter un contrat, et c'est particulièrement vrai dans notre industrie où les termes et les concepts sont très techniques, il importe avant tout de bien définir les termes. Très souvent, ces termes techniques ne sont pas compréhensibles à première vue ni par les usagers, ni par les tribunaux. Dans plupart des licences de logiciel, on préfère le terme «programme» au terme «produit» pour éviter toute implication de matérialité. Pour la même raison, des objets tangibles comme des rubans ou des disques sont d'ordinaire distincts du programmes. Le terme «matériel» remplace d'ordinaire le terme «documentation». Le terme «documentation» est souvent utilisé dans l'industrie, mais on lui préfère le terme «matériel» dans le cas des contrats pour élargir la couverture et éviter la définition technique trop étroite d'un terme comme «documentation». Un autre mot qu'on retrouve souvent dans les contrats de l'industrie, le terme «mise en valeur». Cela comprend les modifications, les améliorations, les remises à jour et autres synonymes couramment utilisés.

[Text]

A typical software licence used in our industry usually includes, in article 1 of the contract, immediately following the section that identifies the parties to the agreement, some definitions. As an example:

For the purpose of this agreement, the following are defined terms:

The term "licensed program" shall mean a licensed information processing program or programs, consisting of a series of instructions or statements which is machine readable.

I think one point that might be noted in connection with that definition is that it says "machine readable," but it does not say that it is in electronic terms. With the developments that are going on in the industry it could be in optical terms or even in biological terms, because there is research going on now in programming microbes to process information. So that the problem of any definition, of course, is to avoid having it become obsolete before it gets printed.

• 0955

Another term that is defined in many of our contracts is the term "licensed materials".

2. The term "licensed materials" shall mean any materials related to the licensed program and provided for use in connection with the licensed program.

3. The term "licensed program and materials" shall mean both the licensed program and licensed materials as defined above.

The term "enhancement" is often defined to mean "any program, any part thereof, or any materials not included in the licensed program and materials at the time of execution of this agreement that is related to the licensed program and materials".

Another term that is often defined is the term "use"—"this shall include copying any portion of the licensed program or licensed materials into the computer or transmitting them to a computer for processing of the instructions, or statements contained in the licensed program or materials".

I participated in the consultation that the Department of Justice and CIPS held early in March in Toronto, and one of the things that was suggested by at least one of the groups there was that the term "use" be defined. I think one of the suggestions that came forward was that it should be to cause the machine to consume a cycle.

There is often a background section in our licensing agreements and contracts where the software company who developed the product wishes to make clear its investment in development. A typical section there might read:

BSA is the developer and owner of the licensed program materials known as "jigger" for performing market evaluations and forecast projections.

[Translation]

Une licence de logiciel typique comprend d'ordinaire dans le premier article du contrat, et tout de suite après le paragraphe qui identifie les parties à l'accord, une liste de définitions. Un exemple:

Aux fins de cet accord, les termes suivants sont définis:

Le terme «programme sous licence» signifie un ou plusieurs programmes de traitement de l'information sous licence, constitués d'une série d'instructions qui sont lisibles par une machine.

La première chose qui ressort de cette définition, c'est qu'il est question de quelque chose qui est «lisible par une machine» sans aucune mention de termes électroniques. Avec les progrès qui sont accomplis actuellement dans l'industrie, il pourrait s'agir de termes optiques, et même de termes biologiques, parce qu'on fait actuellement des recherches sur l'utilisation des microbes pour le traitement de l'information. Dans ces conditions, n'importe quelle définition laisse des problèmes, et en particulier le risque d'être dépassée avant même d'être imprimée.

Un autre terme est souvent défini dans nos contrats: «matériaux sous licence».

2. Le terme «matériaux sous licence» signifie tous matériaux liés au programme sous licence et pouvant être utilisés en conjonction avec le programme sous licence.

3. Le terme «programme et matériaux sous licence» signifie à la fois le programme sous licence et les matériaux sous licence, selon la définition qui précède.

Le terme «mise en valeur» est souvent défini comme étant «tout programme, toute partie de programme, ou tous matériaux ne figurant pas dans le programme ou les matériaux sous licence au moment de l'exécution de cet accord, mais étant lié au programme et aux matériaux sous licence».

Le terme «utilisation» est également souvent défini: «cela comprend la reproduction de toute partie d'un programme sous licence ou de matériaux sous licence dans l'ordinateur, ou leur transmission à un ordinateur pour traitement des instructions, ou phrases contenues dans le programme ou les matériaux sous licence».

J'ai participé aux consultations entre le ministère de la Justice et le CIPS, au début de mars, à Toronto, et un des groupes présents au moins a suggéré que l'on définisse le terme «utilisation». Une des définitions voulait que «utilisation» corresponde à un cycle complet de la machine.

Nos accords de licence et nos contrats comprennent souvent une partie consacrée à l'historique du produit; les fabricants de logiciel qui ont mis au point le produit en profitent pour souligner le rôle qu'ils ont joué dans la mise au point du produit. Je vous cite un article typique:

BSA est le concepteur et le propriétaire d'un programme sous licence connu sous le nom de «jigger», qui sert à effectuer des évaluations de marché et des projections.

[Texte]

Client is now requesting BSA to grant a non-exclusive licence to use the licensed program and materials only in the conduct of client's business.

In software licences there are a number of prohibitive clauses. As an example:

Software licensed by BSA, as provided hereunder, as well as any future enhancements or updates, is furnished to client under a licence for use on a single central processing unit and may not be copied in whole or in part, except for use on such CPU. Any copies made by client for such use must include the BSA software copyright notice. The client shall not provide, or otherwise make available to a third party, any copies or a part thereof in any form, unless authorized in writing by BSA to do so.

Title to and ownership of the software and any unmodified parts thereof shall at all times remain with BSA.

BSA shall have the right to terminate client's licence if client fails to comply with these licence terms and conditions and client agrees, upon notice of such termination, to immediately return or destroy the software and all portions and copies thereof.

There are a number of things that are required that are done by the service company and required of the client in connection with these contracts for computer services. The service company provides the client with an account number, as many user numbers as the client requires for his staff use and a password for each of these user numbers.

On the client's side:

It shall normally be the client's responsibility to supply its own terminal equipment. Such equipment and its installation and compatibility to BSA's computers is subject to acceptance by BSA.

The client accepts sole responsibility for the accuracy and adequacy of its source data, all programs of whatever origin, instructions, procedures and the results obtained therefrom. The client agrees to prepare its program to detect system errors, and to be responsible for establishing proper audit controls, operating methods, appropriate back-up files, back-up programs and check points necessary for the client's intended use of the machines and computer services.

All programs, specifications, routines or techniques which are disclosed by BSA to client pursuant to this agreement shall remain the property of BSA and the client will not disclose or make available the same to any third party without prior written consent of BSA.

Usually there are clauses on infringement in these contracts, too, where the client agrees to hold BSA harmless from any claims by third parties pertaining to infringement of copyrights or otherwise arising out of the processing by BSA of

[Traduction]

Le client demande maintenant à BSA de lui accorder un permis non exclusif d'utilisation du programme et des matériaux sous licence, uniquement dans le cadre des affaires courantes du client.

Dans les licences de logiciel, il y a un certain nombre d'interdictions. Un exemple:

Le logiciel sous licence BSA, conformément aux dispositions qui suivent, et aux termes de toutes mises en valeur et améliorations futures, est fourni au client aux termes d'une licence pour utilisation sur une unité centrale de traitement unique, et ne peut être reproduit en partie ou en totalité, à l'exception de l'utilisation sur cette unité centrale. Toute copie faite par un client dans le cadre de ces dispositions doit porter un avis de *copyright* pour le logiciel appartenant à BSA. Le client ne peut fournir ou mettre à la disposition d'une tierce partie des copies totales ou partielles, sous une forme quelconque, sans une autorisation écrite de BSA.

Les titres de propriété sur le logiciel et sur ses parties non modifiées sont la propriété exclusive de BSA.

BSA a le droit d'annuler la licence d'un client si celui-ci ne se conforme pas aux conditions de la licence, et le client accepte, s'il reçoit un avis d'annulation de cette nature, de remettre immédiatement à BSA le logiciel et toutes les parties et copies qui ont été faites, ou de les détruire.

La compagnie de services et le client sont tenus de respecter un certain nombre de dispositions relatives à ces contrats de services informatiques. La compagnie de services donne au client un numéro de compte, et également des numéros pour le personnel du client, ainsi qu'un mot de passe pour chacun de ces numéros.

Les obligations du client:

D'ordinaire, c'est le client qui doit fournir le matériel terminal. Ce matériel, son installation et sa compatibilité avec les ordinateurs de BSA sont sous réserve de l'approbation de BSA.

Le client accepte la responsabilité exclusive de l'exactitude et de la qualité des sources de données, de tous les programmes, quels que soient leur origine, instructions, procédures, ainsi que des résultats obtenus. Le client accepte de préparer ses programmes pour déceler les erreurs de système, et il assume également la responsabilité de la mise en place de contrôles de vérification suffisants, de méthodes de fonctionnement, de dossiers de soutien, de programmes de soutien et de vérifications nécessaires dans le cadre de l'utilisation, par le client, des machines et des services informatiques.

Tous les programmes, spécifications, systèmes ou techniques qui sont communiqués par BSA à un client conformément à cet accord sont la propriété exclusive de BSA, et le client s'engage à ne pas les communiquer à une tierce partie sans la permission écrite de BSA.

D'ordinaire, il y a des clauses sur le non-respect de ces contrats où le client accepte de renoncer à toute poursuite contre BSA par des tierces parties pour non-respect des droits d'auteur, ou autres, à la suite de traitements effectués par BSA

[Text]

proprietary systems and programs supplied by the client to BSA.

• 1000

I noticed in previous testimony before this subcommittee, and I believe it was Professor Palmer who said that there was no record of any software ever having been copyrighted in Canada. I believe there have been some copyrighted in the States. But I notice that most people who have programs seem to include a warning on their program to say that they own the copyright to this program. Maybe this is in anticipation of being able to copyright.

Computer service company responsibility regarding client data: With respect to financial, statistical, personnel, technical data relating to the client's business which is confidential, is clearly so designated by the client and which is submitted to BSA by the client in the course of performing services hereunder, BSA will instruct BSA personnel to keep such information confidential by using the same care and discretion that they use with similar data which BSA designates as confidential. However, BSA shall not be required to keep confidential any data which is, or becomes, publicly available, is already in BSA's possession, is independently developed by BSA outside the scope of this agreement, or is rightfully obtained from third parties.

CADAPSO's legal advisers have stated that a licensed program and materials which BSA—say, the member company—considers to be proprietary and a trade secret, will be treated by the courts as a trade secret if BSA's behaviour towards the licensed program and materials shows an effort to preserve the secret.

A typical article in some of our contracts covers the way that the client is required by the licence agreement to preserve BSA's trade secrets—namely the institution of security measures, an acknowledgement of confidentiality, or a restriction on copying the licensed program and materials.

A typical agreement may have a section such as this on security. Here the client will protect the confidential nature of the licensed program and materials by establishing written guidelines with respect to its employees and other persons permitted access to the licensed program and materials to prevent the licensed program and materials from being acquired by unauthorized persons. The guidelines shall be at least as strict as the BSA guidelines which are attached.

Now I have attached to the back of our submission a copy of guidelines put out by a government department. Many of our companies provide computing services to government departments, and they have security requirements which are normally sent out with the invitations to bid on a contract, or the request for proposals. So I have attached a typical one as Appendix B to this submission.

[Translation]

à partir de systèmes et de programmes privés fournis par le client à BSA.

Dans d'autres témoignages que vous avez entendus, j'ai lu que le professeur Palmer, je crois, vous a dit qu'aucun logiciel n'a jamais été sous *copyright* au Canada. Par contre, il y en a eu aux États-Unis. Cela dit, la plupart des gens qui possèdent des programmes font une mise en garde sur le programme, précisant leurs droits d'auteur sur le programme. C'est peut-être en attendant d'obtenir le *copyright*.

Les compagnies de services informatiques ont des responsabilités envers les données appartenant au client: pour les données financières, statistiques, techniques et les données sur le personnel de leur client qui sont confidentielles, les données que le client a désignées spécifiquement comme étant confidentielles avant de les soumettre à BSA pour l'accomplissement d'un service, BSA doit prévenir son personnel de tenir ces informations confidentielles et de garder les mêmes précautions et la même discrétion que pour des données comparables appartenant à BSA et désignées comme étant confidentielles. Toutefois, BSA ne peut être tenue de garder confidentielles des données qui, après avoir été communiquées à BSA, deviennent publiques par des moyens échappant au contrôle de BSA, ou sont communiquées légalement à une tierce partie.

Les conseillers juridiques de CADAPSO ont déterminé qu'un programme et des matériaux sous licence que BSA—disons la compagnie membre—considère comme lui appartenant et comme constituant un secret commercial doivent être traités par les tribunaux comme un secret commercial si le comportement de BSA face au programme et aux matériaux sous licence prouve qu'un effort a été fait pour garder le secret.

Un article typique, dans un de nos contrats, couvre la façon dont le client est tenu, conformément à l'accord de licence, de conserver les secrets commerciaux de BSA. Il s'agit de la mise en place de mesures de sécurité, d'une reconnaissance du caractère confidentiel des données, ou de restrictions sur la reproduction de programmes et de matériaux sous licence.

Un accord typique peut contenir un paragraphe comme celui-ci sur la sécurité. Dans ce cas, un client protège la nature confidentielle du programme et des matériaux sous licence en rédigeant des directives écrites à l'intention de ses employés et de toute autre personne qui aura accès au programme et aux matériaux sous licence, pour éviter que le programme et les matériaux sous licence ne soient communiqués à des personnes non autorisées. Les directives doivent être au moins aussi sévères que les directives de BSA qui sont annexées.

Maintenant, j'ai ajouté à la fin de notre exposé un exemple de directives préparées par un ministère du gouvernement. Très souvent, nos compagnies assument des services d'informatique pour le compte de ministères du gouvernement, et d'ordinaire, les appels d'offres sont accompagnés d'une série d'exigences en matière de sécurité. Je vous ai donc soumis une liste typique; c'est l'annexe B de ce mémoire.

[Texte]

One of the things that is usually specified is that the client will not create, attempt to create, or re-create, or permit or help others to re-create, the source code from the licensed program and materials furnished pursuant to this agreement. What is provided to the client by the service company is the object code, and most companies or some companies build into these programs what they might call a bug or a sleeping bug that can be activated if the person using the program tries to modify it in some unauthorized way. So this is another security measure that is built into the program itself; that it may self-destruct or cause things to happen which would indicate that the person using the program has attempted to modify it.

Thinking in terms of the physical security and program storage, a typical clause might be: Client will store the licensed program and materials in a safe place and record the name of each person having access to the licensed program and materials.

• 1005

A client will promptly notify BSA in writing in the event of any unauthorized person's having access to the licensed program and materials. I mentioned that a number of our companies have contracts with the Canadian government. There are clauses usually right at the beginning of the request for proposals and a typical one might be something like this: Bidders' facilities may be inspected for compliance with these requirements by the Security Service Branch of the Department of Supply and Services or the security, evaluation and inspection team, SEIT, of the RCMP at any time during the procurement process.

The successful bidder is also subject to inspection at any time during the life of any resultant contract. The contractor shall be responsible for establishing a screening program for applicants and employees who, through their employment with the organization, may have access to government sensitive information. Such programs should address the following criteria: *a*) verification of identification; *b*) verification of academic and technical educational qualifications; *c*) record of previous employment; *d*) reference checks, minimum of two; *e*) credit bureau check; *f*) bonding, where applicable; *g*) pre-employment interview; and *h*) signing of Department of Supply and Services form 1815, oath of secrecy. So these are some of the security requirements and precautions that are required of our member companies when they do business with government departments through the contracting process with the Department of Supply and Services.

Back in 1981, CADAPSO submitted a lengthy brief to the transport or data flow task force of the Department of Communications. In this brief, we highlighted the pertinent issues that affect computer services companies in Canada. One of CADAPSO's stated concerns was, and still is, the protection of proprietary data bases and software packages. Authorized

[Traduction]

Une des choses qui est d'ordinaire précisée, c'est que le client ne cherchera pas à créer, à recréer, ou à aider une tierce partie à recréer le code source du programme et des matériaux sous licence fournis conformément à cet accord. Ce que la compagnie de services met à la disposition du client, c'est le code objet, et la plupart des compagnies, ou du moins certaines d'entre elles, ajoutent dans ces programmes ce qu'elles peuvent appeler un «microbe», ou microbe dormant, qui peut être réveillé si la personne qui utilise le programme cherche à le modifier d'une façon non autorisée. Voilà donc une autre mesure de sécurité inscrite dans le programme même. Dans ces circonstances, il y a autodestruction du programme, ou encore un signal d'alarme quelconque qui prévient que la personne qui utilise le programme a cherché à le modifier.

Je passe maintenant à la sécurité matérielle et à l'entreposage des programmes; un article typique: le client entrepose le programme et les matériaux sous licence dans un endroit sûr et enregistre le nom de toutes les personnes qui ont accès au programme et aux matériaux sous licence.

Un client avertit BSA immédiatement par écrit si une personne non autorisée a eu accès à un programme et des matériaux sous licence. J'ai déjà dit qu'un certain nombre de nos compagnies avaient des contrats avec le gouvernement canadien. D'ordinaire, tout au début du document d'appel d'offres, il y a un article qui peut être rédigé de cette façon: les installations des personnes qui font une offre peuvent être inspectées pour déterminer si elles sont conformes aux exigences de la Direction de la sécurité du ministère des Approvisionnement et Services ou de l'équipe de la GRC chargée de la sécurité, de l'évaluation et de l'inspection, et ce, à n'importe quelle étape du contrat d'approvisionnement.

La compagnie dont l'offre aura été retenue peut également être inspectée à n'importe quel moment pendant la durée du contrat. L'entrepreneur est responsable de la mise en place d'un programme de sélection des employés qui, dans le cadre de leurs activités au sein de l'organisation, pourraient prendre connaissance d'informations confidentielles du gouvernement. Ces programmes doivent respecter les critères suivants: *a*) vérification d'identité; *b*) vérification des qualifications universitaires et techniques; *c*) emplois antérieurs; *d*) vérification des références; minimum de deux, *e*) vérification auprès du Bureau de crédit; *f*) assermentation le cas échéant; *g*) entrevue aux fins de recrutement; et *h*) signature du formulaire 1815 du ministère des Approvisionnement et Services, serment de secret. Voilà donc certaines conditions et précautions de sécurité qui sont exigées de nos compagnies membres lorsqu'elles font affaires avec des ministères du gouvernement par l'entremise des services d'approvisionnement du ministère des Approvisionnement et Services.

En 1981, CADAPSO avait préparé un long mémoire pour le groupe de travail chargé d'étudier la circulation des données et les transports pour le compte du ministère des Communications. Dans ce mémoire, nous avons relevé les problèmes qui affectaient les compagnies de services informatiques au Canada. Une de nos préoccupations était, et est toujours, la

[Text]

users have the inherent ability to copy and possibly distribute or sell unauthorized copies of data and software, and this abuse of acquisition or use of information is not considered theft under the Canadian law as it now stands. Theft is defined in the Criminal Code as only that activity which results in the owner being deprived of the rightful use of the tangible property stolen from him; and data and software have not been defined in the law and they are not considered tangible property. As I mentioned earlier, most of our contracts refer to programs rather than products for that reason.

If a copy is made of a data base or a software program, the owner has not been deprived by that act of the use of the data base or software, although he may, of course, be deprived of anticipated revenue through future unauthorized use of his data and programs.

The Canadian Copyright Act may prohibit the unauthorized copying of printed computer output, but its current provisions may not cover the copying of information stored in electronic form in computer memories or related accessories. And the CADAPSO brief to the Department of Communications made the point that unauthorized copying of data is important from a trans-border data flow point of view, as this data can be transported or transmitted outside of Canada very easily, of course, through satellite communication, and can be used in a totally uncontrollable manner. Our recommendation to the Department of Communications task force was that software, services, programs must be properly defined in law and the law must provide protection to authors of programs, software manufacturers, service companies. The government should review the Copyright Act and make provisions for this new technology.

Another concern of our association, which was contained in this brief to the Department of Communications, was followed in April of 1982 by a similar brief that was submitted to the Department of Industry, Trade and Commerce. In this we recommended a legal definition of computer services.

• 1010

International trade agreements recognize that the dumping of products by one country into another, at prices not consistent with prices charged in the country of manufacture, is an undesirable practice. And international dumping laws have been used successfully on many occasions, both in Canada and in other countries. But in general, Canadian laws relating to dumping have no effect on the service industries. The nature of services is such that they are usually performed by an individual, and as such they are not exportable and not dumpable. In general this is true but the major exception to this rule, I think, is the computer services business.

Computer services are manufactured, if I can use that word, by computers with the aid of large numbers of highly capable,

[Translation]

protection des bases de données privées et des systèmes de logiciel. Les usagers non autorisés peuvent facilement reproduire et même distribuer ou vendre des copies non autorisées de données et de logiciel et à l'heure actuelle, cette activité n'est pas considérée comme un vol par la loi canadienne. Dans le Code criminel, le vol est défini comme étant une activité qui prive le propriétaire légal de l'utilisation légale d'un bien tangible qui lui a été volé. La loi n'a pas encore défini les données et le logiciel qui ne sont toujours pas considérés comme un bien tangible. Comme je l'ai déjà dit, c'est pour cette raison que la plupart de nos contrats parlent de programmes et non pas de produits.

Lorsqu'une base de données ou un programme logiciel sont reproduits, la propriétaire ne se trouve pas privé d'utiliser cette base de données ou logiciel même si très souvent, il est privé des revenus qu'il s'attendait à réaliser grâce à l'utilisation de ces programmes.

La Loi sur le droit d'auteur peut interdire la reproduction non autorisée d'imprimés d'ordinateur mais ses dispositions actuelles ne tiennent pas forcément compte de la reproduction d'informations entreposées sous forme électronique dans des mémoires d'ordinateur ou autres accessoires. Dans son mémoire destiné au ministère des Communications, CADAPSO avait observé que la reproduction non autorisée de données constituait un problème grave du point de vue de la circulation des données à travers les frontières, puisqu'il était très facile d'expédier ou de transmettre ces données à l'extérieur du Canada, par satellite, ce qui rendait tout contrôle impossible. A l'époque, nous avions recommandé au groupe de travail du ministère des Communications de définir en droit le logiciel, les services et les programmes et d'assurer une protection des auteurs de programmes, des fabricants de logiciel et des compagnies de service. Il faudrait que le gouvernement révisé la Loi sur le droit d'auteur et adopte des dispositions pour tenir compte de cette nouvelle technologie.

Dans ce même mémoire à l'intention du ministère des Communications, qui avait d'ailleurs été suivi d'un mémoire similaire à l'intention du ministère de l'Industrie et du Commerce en 1982, nous exprimions d'autres préoccupations. En particulier, nous avions recommandé une définition légale des services d'ordinateur.

Les ententes commerciales internationales condamnent le dumping de produits par un pays dans un autre pays à des prix qui ne sont pas compatibles avec les prix en cours dans le pays de fabrication. Très souvent, le Canada et d'autres pays ont invoqué avec succès des lois internationales sur le dumping. Cela dit, en règle générale, les lois canadiennes sur le dumping n'ont pas d'effet sur les industries de services. La nature de ces services est telle que d'ordinaire ce sont des particuliers qui les assurent et, à ce titre, ni ils ne sont exportables ni ils ne peuvent faire l'objet de dumping. La plupart du temps, cela est vrai, mais il y a une exception majeure: le secteur des services informatiques.

Les services informatiques sont fabriqués, si l'on peut dire, par des ordinateurs avec l'aide d'un personnel considérable et

[Texte]

highly trained and highly paid, professional computer experts. But since the results of this service manufacturing process can be delivered electronically anywhere in the world, it is entirely possible to export and dump computing services in another country. A company which has developed a significant software package—and these often run to millions of dollars—could charge only, say, 50% of its domestic charges in a foreign country. And this would provide marginally costed revenues against which none of the original investment costs need to be charged.

As a result of these considerations a recommendation was made to the Department of Industry, Trade and Commerce, in our brief to them, that services of the nature produced by the electronic data processing service industry should be defined in the same manner as a tangible product is defined, so that the anti-dumping laws may be applied to the dumping of services from foreign countries into Canada.

At the national consultation in Toronto, in March, I participated in the discussions on the first day and was asked to make a statement on behalf of CADAPSO regarding some suggestions I had made the previous day about the definitions of data and information. And in the group that I sat with, I made the point that there should be a distinction made between data and information. This was a point that CADAPSO had made in its submission to the Trans-Border Data Flow Task Force. I said to the group at the time that I wished at that time that Professor Gotlieb, of the University of Toronto Department of Computer Science, had been in my group, because he had spoken just before I did at this conference and came up with some definitions that were very similar to the ones that I had proposed.

Data, of course, exists totally independent of computers, and one way of describing it is as the symbolic representation of a concept. But what is in computers is stored data. It is data that has been encoded and stored in a computer system or a component part of a computer system. And I would like to suggest that the distinction needs to be made between that, although the machine cannot make the distinction because the electrical or optical or whatever other impulses are in the machine all look the same to the machine, although they can be treated differently.

Information is the representation of the intellectual content which results from processing data in a computer system by means of a computer program. And as I mentioned earlier, although a lot of people have recommended that nothing be defined, I think if we are to deal with this appropriately in the law that some of these things need to be defined. Dr. Gotlieb, as I mentioned, had spoken of his definitions of data and information, and he also proposed that they should be defined separately. He said that he had just written a book called *The Economics of Computers—Costs, Benefits, Policies, Strategies*, and his definitions are in a chapter in that book on the value of information.

[Traduction]

très qualifié, très bien payé, les professionnels de l'informatique. Cela dit, étant donné que les résultats de ce processus de fabrication d'un service peuvent être transmis électroniquement n'importe où dans le monde, il est parfaitement possible d'exporter et de faire du dumping de services d'ordinateurs dans un autre pays. Une compagnie qui a un logiciel considérable... ce qui représente souvent des millions de dollars... peut parfaitement ne demander que 50 p. 100 de la valeur domestique du service à un autre pays. Une fois les coûts d'investissement amortis, ces revenus marginaux sont encore très rentables.

Pour tenir compte de ces considérations, nous avons fait une recommandation au ministère de l'Industrie et du Commerce et proposé que les services rendus par l'industrie de traitement électronique des données soient définis de la même façon qu'un produit tangible et définis pour que les lois anti-dumping puissent s'appliquer au dumping de services d'un pays à l'autre.

Lors de la consultation nationale en mars dernier à Toronto, j'ai participé aux discussions du premier jour et, à cette occasion, on m'avait demandé de donner l'opinion de l'ACOSI sur les suggestions faites la veille pour la définition des données et de l'information. J'avais alors expliqué au groupe dans lequel je me trouvais, qu'il faudrait faire une distinction entre données et information. C'est précisément ce qu'avait expliqué l'ACOSI dans son mémoire au groupe de travail sur la circulation des données outre-frontières. À cette occasion, j'avais dit que j'aurais aimé que le professeur Gotlieb, du département d'informatique de l'Université de Toronto, fasse partie de mon groupe, parce que, juste avant cette conférence, à l'occasion d'une causerie, il avait donné des définitions qui ressemblaient de très près à celles que je proposais.

Les données, évidemment, sont une entité totalement indépendante de l'ordinateur et on peut dire qu'il s'agit de la représentation symbolique d'un concept. Ce qui se trouve dans l'ordinateur, ce sont des données entreposées. Ce sont des données qui ont été codées et entreposées dans un système d'ordinateur ou une composante d'un système d'ordinateur. À mon avis, il faudrait faire cette distinction que, même si la machine ne peut pas faire la distinction puisque, pour elle, toutes les impulsions, qu'elles soient électriques, optiques ou autres se ressemblent, cela n'empêche qu'il faudrait les traiter différemment.

L'information, c'est la représentation d'un contenu intellectuel qui est la résultante du traitement de données dans un système d'ordinateur au moyen d'un programme d'ordinateur. Comme je l'ai déjà dit, beaucoup de personnes pensent qu'il ne faut rien définir, mais, pour ma part, je pense que si nous voulons aligner la loi sur les progrès accomplis dans ce domaine, il faut absolument apporter certaines définitions. Comme je vous l'ai dit, le Dr Gotlieb a proposé des définitions des données et de l'information ajoutant que ces définitions devaient être distinctes. Il a dit qu'il venait d'écrire un livre intitulé *«The Economics of Computers—Costs, Benefits, Policies, Strategies»*, (Lois économiques des ordinateurs—Coûts, avantages, politiques, stratégies); ces définitions

[Text]

I have attached to our submission a kind of bibliography—quite a list of articles that I have pulled out of books that I have consulted on the subject of computer crime. One that has often been referred to is by Donn Parker. Another list that comes from an encyclopedia of computer science and engineering which we have in our office, and another book that I consulted, called *Foosles and and Frauds*.

We have also attached the security recommendations that are put out by a typical government department. I hope some of this will be helpful to you in your deliberations, and I would like to turn the presentation over to Wayne Kay who is the Ottawa Manager of Datacrown. Datacrown made a submission to the national consultation in Toronto, and Mr. Kay is here to talk about that.

The Chairman: If you will excuse me. Mr. Robinson, will take the Chair. I have to report to the main committee and they are holding a meeting at the same time, so I will be joining the other group. It is on the same subject. Mr. Robinson will proceed.

The Acting Chairman (Mr. Robinson, (Etobicoke—Lakeshore)): All right, let us continue with Mr. Kay then. You have a presentation to make for Datacrown.

Mr. D. W. Kay (Manager, Ottawa District and ADP Systems, Datacrown Inc.): As Mr. Boire mentioned recently Datacrown, as a member of CADAPSO made a submission, which was prepared by our counsel, to the Department of Justice, the Canadian Information Processing Society and the National Consultation on Computer Abuse. I reference that, which is our submission, as an appendix to the CADAPSO submission today.

Our particular point that we have been making with various committees and other members, is to determine the best methods of preventing unauthorized acquisition, disclosure or use of information knowledge or ideas stored in computer systems. There has been a lot of discussion on this point and therefore we very strongly support the activities of this committee and the member's bill.

This paper does not deal with esoteric topics such as what is property, whether or not information is property, or whether or not the exchange of information in our society is beneficial. Instead we have restricted ourselves for the purpose of this discussion to assume that there are property rights in information knowledge and ideas and that those property rights are entitled to be protected. As a company and as one of the major service companies in this country we feel we have a very significant interest in that, as do our clients.

In our society, property rights are protected through the legal system either by means of criminal law such as the Criminal Code, or civil law, such as a lawsuit for damages.

[Translation]

figurent dans un chapitre de ce livre consacré à la valeur de l'information.

• 1015

J'ai annexé à notre exposé une sorte de bibliographie, en fait une liste d'articles—de livres que j'ai consultés au sujet des infractions informatiques. J'ai fait de nombreuses références à l'un de ces articles, celui de Donn Parker. Je vous donne aussi une autre liste—d'une encyclopédie sur les sciences informatiques et de génie que nous avons dans notre bureau ainsi que le titre d'un autre livre que j'ai consulté «*Foosles and Frauds*» (bâclages et fraudes).

Vous avez également une liste des recommandations typiques de sécurité d'un ministère du gouvernement. J'espère que ces documents vous seront d'une certaine utilité pour vos délibérations et maintenant, j'aimerais donner la parole à Wayne Kay, le gérant de Datacrown pour la région d'Ottawa. Datacrown a fait un exposé à la consultation nationale de Toronto et M. Kay est ici pour vous en parler.

Le président: Veuillez m'excuser; M. Robinson va assurer la présidence. Je suis obligé d'aller au comité principal qui se réunit en ce moment et qui discute justement de ce sujet. M. Robinson va continuer.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien, monsieur Kay, allez-y. Vous avez un exposé au nom de Datacrown.

M. D. W. Kay (gérant, district d'Ottawa et système ADP, Datacrown Inc.): Comme M. Boire vous l'a dit, en sa qualité de membre de CADAPSO, Datacrown a fait récemment un exposé, dont la préparation avait été confiée à notre avocat, devant la Société canadienne du traitement de l'information à l'occasion de la consultation nationale sur les abus en informatique organisée par le ministère de la Justice. Cet exposé est d'ailleurs annexé à l'exposé de CADAPSO.

Notre principal souci, c'est ce que nous avons dit à plusieurs comités et à d'autres membres, est de déterminer les meilleurs moyens de prévenir des acquisitions non autorisées, ou l'utilisation d'informations, de connaissances ou d'idées entreposées dans des systèmes d'ordinateur. C'est un problème qui a fait l'objet de nombreuses discussions et par conséquent, nous sommes tout à fait en faveur des activités de ce comité et de la teneur du bill.

Cet exposé ne traite pas de sujets ésotériques tels que la nature des propriétés, la question de savoir si l'information constitue une propriété et celle de savoir si l'échange d'informations dans notre société est une chose positive. Au lieu de cela, nous nous en sommes tenus à cette assumption qu'il existe des droits de propriété sur l'information et sur les idées et que ces droits de propriété doivent jouir d'une certaine protection. En notre qualité de compagnie, de compagnie de services importante dans ce pays, nous nous sentons directement concernés par cette question, comme nos clients.

Dans notre société, les droits de propriété sont protégés par le système juridique, qu'il s'agisse du droit criminel, c'est-à-dire du Code criminel, ou du droit civil, les poursuites pour

[Texte]

Both the criminal law and civil law have advantages and disadvantages as methods to prevent abuse of computer systems.

Generally, criminal sanctions are reserved for those individuals who have committed more flagrant abuses of property rights or violence to the individual. The authorities must be convinced that there are reasonable and probable grounds to suspect that a particular individual has committed an offence.

Assuming that there had been a sophisticated abuse of a computer system, and assuming that such abuse was contrary to the criminal law, it would be necessary to first explain the nature of the abuse to an individual having knowledge and experience of computer systems and, secondly, to generate sufficient interest in that individual to prevail upon the authorities to prosecute a perpetrator of the alleged abuse. From a practical point of view, even assuming one can convince the authorities to prosecute, one wonders whether or not a subtle abuse of a computer system would capture the attention of a judge or jury to the same extent as alleged crimes of other forms of property rights and violence to an individual.

Another significant disadvantage in the utilization of the criminal law in an attempt to prevent the abuse of computer systems is the onus on proof which must be overcome by the Crown in order to obtain a conviction. In a criminal prosecution, the individual accused of the criminal offence is presumed innocent until proven guilty and that individual is not required to testify against himself.

• 1020

Perhaps more importantly, in a criminal prosecution the Crown must demonstrate to the judge or jury that the accused is guilty beyond a reasonable doubt. Those procedural safeguards have been incorporated into the criminal law so as to protect the rights and freedoms of members of society generally. However, by reason of those same safeguards, the criminal law is perhaps an inefficient method whereby to prevent the more subtle abuse of computer systems; and this is of particular concern.

It is also submitted that the more flagrant aspects of computer abuse must be prohibited by criminal law. At present, there are certain sections of the Criminal Code to which resort might be had with respect to certain aspects of computer abuse. In particular, the following sections of the Criminal Code may be applicable: Section 283, general offences of theft; Section 312, possession of property obtained by crime; Section 361, falsely assuming the identity of another; Section 387.(1)(b), (c) and (d), destruction of property or obstruction of lawful use thereof.

It is submitted, however, that the above-noted sections do not adequately prohibit the unauthorized acquisition, disclosure or use of information, knowledge or ideas stored in the computer systems. Instead, an amendment to the Criminal Code might be considered in order to prohibit such forms of abuse. In particular, Section 287 of the Criminal Code provides that it is a criminal offence if one:

[Traduction]

dommages et intérêts. Les deux méthodes de prévention des abus de système d'ordinateur, celles du droit criminel et du droit civil ont leurs avantages et leurs inconvénients.

En règle générale, les sanctions criminelles sont réservées aux individus qui ont commis les abus les plus flagrants contre des droits de propriété ou qui se sont rendus coupable de violence contre un individu. Les autorités doivent être convaincues qu'elles ont de bonnes raisons de soupçonner un individu d'avoir commis une infraction.

Supposons que quelqu'un ait abusé d'un système d'ordinateur, d'une façon à la fois complexe et contraire au droit criminel; il faudrait d'abord expliquer la nature de l'abus à une personne qui possède une certaine expérience des systèmes d'ordinateur et ensuite, il faudrait réussir à convaincre cette personne de la nécessité de convaincre les autorités d'entamer des poursuites. Du point de vue pratique, même si l'on arrivait à convaincre les autorités d'entamer des poursuites, il faut encore se demander si les infractions les plus subtiles réussiraient à intéresser un juge ou un jury au même titre qu'un crime plus conventionnel, violation de propriété ou violence envers une personne.

Autre inconvénient grave du recours au droit criminel pour décourager les infractions relatives à des systèmes d'ordinateur, c'est que le fardeau de la preuve repose sur la Couronne si l'on veut établir la culpabilité. Dans des poursuites criminelles, la personne accusée d'une infraction criminelle est présumée innocente tant qu'elle n'a pas été prouvée coupable et, à ce titre, n'est pas tenue de témoigner contre elle-même.

Mais, plus important peut-être, c'est que la Couronne, dans des poursuites criminelles, doit prouver au juge ou au jury que l'accusé est coupable sans l'ombre d'un doute. Ces garanties de procédure ont été codifiées dans la loi pénale, afin de protéger, d'une façon générale, les droits et libertés des membres de la société. Toutefois, en raison même de ces protections, la loi pénale constitue peut-être un instrument inefficace pour empêcher les infractions plus subtiles des systèmes d'informatique, et c'est ce qui nous préoccupe beaucoup.

On a également proposé que les infractions les plus flagrantes relatives aux ordinateurs soient interdites par le droit pénal. À l'heure actuelle, il existe certains articles du Code criminel qu'il est possible d'invoquer pour certains aspects d'infractions relatives aux ordinateurs, en particulier l'article 283, vol (général); l'article 312, avoir en sa possession des biens criminellement obtenus; l'article 361, supposition intentionnelle de personne; l'alinéa 387.(1) b), c) et d), rend un bien dangereux, ou empêche, interrompt ou gêne l'emploi, la jouissance ou l'exploitation légitime d'un bien.

On a toutefois fait état du fait que les articles susmentionnés n'interdisent pas de façon adéquate l'acquisition non autorisée, la communication ou l'utilisation d'informations, de connaissances ou d'idées emmagasinées dans les systèmes informatisés, et l'on envisage un amendement au Code criminel qui interdirait ce genre d'infraction. L'article 287 du Code criminel, entre autres, stipule:

[Text]

fraudulently, maliciously or without colour of right, uses any telecommunication facility or obtains any telecommunication service.

An amendment to Section 287 might be considered so as to provide a prohibition against fraudulent, malicious or without colour of right use of any computer system. Such an amendment might prove effective in controlling flagrant examples of abuses of computer systems by acting as a deterrent to individuals who might otherwise consider an unauthorized use of a computer system.

With respect to the more subtle and sophisticated abuses of computer systems, which will more than likely become prevalent, the civil law may be a more useful tool than the criminal law. In civil litigation, the individual litigant—presumably, one whose proprietary rights have been abused—would pursue the abuser of those rights. As a result, the litigant who initiates the suit would be more keenly interested in the outcome of the action.

Unlike criminal law, civil law is usually more flexible in that the statute could be more easily amended to keep abreast of the advances in computer technology. As well, the safeguards of civil law are not as rigorous. For example, the onus in any civil litigation is on the plaintiff to prove his case on the balance of probabilities as opposed to the onus on the Crown in the criminal law to prove the accused guilty beyond a reasonable doubt.

A further suggestion which the government might consider, in addition to the amendment to the Criminal Code, might be the passage of a statute to regulate these rights which might be threatened by an unauthorized acquisition of information. An example of such a statute designed to protect the proprietary rights in information, knowledge and ideas is the Copyright Act. Both levels of government may wish to consider legislation of a similar nature designed to prevent the abuse of computer systems. Such legislation might provide double or treble damages for anyone found to have acquired, disclosed or used information, knowledge or ideas without authorization.

In summary, it is submitted that both the criminal law and the civil law are required in order to fully protect the proprietary rights in information, knowledge or ideas stored in computer systems. It is suggested that the criminal law be used to prohibit the flagrant abuse of those systems through an amendment to the Criminal Code as outlined. It is further suggested that the more subtle and sophisticated forms of computer abuse might be more easily dealt with through the civil law, and in particular, the passage of a civil statute designed to protect those proprietary rights.

That is the submission made by Datacrown, a member of CADAPSO, to the Department of Justice.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have attached to your notes another section,

[Translation]

commet un vol quiconque, frauduleusement, malicieusement ou sans apparence de droit... se sert d'installations ou obtient un service en matière de télécommunication.

Pour interdire un tel usage, il serait possible d'envisager un amendement à l'article 287, amendement qui pourrait s'avérer efficace contre les abus flagrants des systèmes informatisés, en servant de dissuasion à des personnes qui pourraient autrement envisager d'utiliser un ordinateur de façon non autorisée.

En ce qui concerne les abus plus subtils et plus raffinés des systèmes informatisés, qui risquent fort de devenir plus fréquents, le droit civil constituerait peut-être un outil plus utile que le droit pénal. En litigation civile, le plaideur individuel—au droit de propriété duquel il a sans doute été porté atteinte—poursuivrait en justice celui qui a enfreint ces droits. En conséquence, le plaideur qui entame les poursuites s'intéresserait davantage à l'issue du procès.

À la différence du droit pénal, le droit civil est généralement plus souple, en ce sens que la loi pourrait plus facilement être modifiée pour tenir compte de l'évolution technologique de l'informatique. En outre, les protections du droit civil ne sont pas aussi rigoureuses. C'est ainsi que dans tout procès au civil, c'est au plaignant de faire la preuve de son bon droit, dans l'évaluation des probabilités, alors qu'au pénal, c'est la Couronne qui a le fardeau de la preuve et qui doit parvenir à la quasi-certitude que l'accusé est coupable.

Outre l'amendement au Code criminel, le gouvernement pourrait également envisager d'adopter une loi réglementant ces droits auxquels l'acquisition illégitime d'informations pourrait porter préjudice. La Loi sur le droit d'auteur constitue l'exemple d'une loi ainsi conçue pour protéger les droits du propriétaire d'informations, de connaissances, et d'idées. Les deux paliers de gouvernement pourraient vouloir envisager une législation similaire, conçue pour empêcher les infractions relatives aux ordinateurs. Une telle législation pourrait prévoir des dommages et intérêts doubles ou triples pour toute personne dont il aurait été prouvé qu'elle avait acquis, divulgué ou utilisé des informations, connaissances ou idées sans autorisation.

Il est proposé en résumé qu'il soit possible d'avoir recours au droit pénal et au droit civil afin de pleinement protéger les droits de propriété des informations, connaissances ou idées, emmagasinées dans les ordinateurs. Il est proposé que le droit pénal soit utilisé pour interdire l'abus flagrant de ces systèmes, en apportant au Code criminel un amendement comme celui que nous avons proposé. Il est également proposé que les formes plus subtiles et raffinées d'infractions relatives aux ordinateurs pourraient être traitées plus facilement en droit civil, en particulier en adoptant une loi destinée à protéger ces droits.

C'est la proposition faite par Datacrown, membre de l'ACOSI, au ministère de la Justice.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez mis en annexe à vos notes un autre

[Texte]

entitled "Datacrown Submission to National Consultation on Computer Abuse".

Mr. Kay: I attached those as additional information, if we were going to actually give a . . . Essentially, that just capsulizes what is in our written submission.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right. I will get started on the questioning, then, as the first questioner. I will ask Mr. Boire some questions first.

• 1025

I note, Mr. Boire, on the first page of your notes you indicated that member companies cover almost all aspects of computer services. Later on in your paper, you talked about the security that is provided by your organization. I am wondering about the security that is provided by the people who make the equipment.

Mr. Boire: Our association has the major equipment manufacturers as associate members; people like Control Data, Digital, IBM are associate members of our association. I think you had Mr. John Dean of IBM before your committee some time ago; he talked about some of the security provisions they make available to their customers. Of course, making them available and whether or not the customer uses them is another question. This is true, of course, in our industry. We can make certain security requirements on the client; we can make certain information available to him, but of course it is difficult to enforce it or to know in detail whether they are using it.

I think a lot of the difficulties that arise probably arise through human weakness or carelessness. People tend to be careless sometimes about their terminals. They leave them on, or maybe write their password on something that somebody else can pick up. There are many ways in which systems can be defeated through that kind of carelessness on the part of the user.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You talk about the difficulty of enforcement of the security provisions that might be provided, but what about the cost of these security provisions? Is there a substantial cost involved?

Mr. Boire: I think I would prefer to turn that one over to Dwayne, who is managing the Ottawa branch of a large company that is operating the systems.

Mr. Kay: Essentially, I think security provisions, both on the hardware and software sides of things, are very adequate today. One normally finds that security is looked upon by the end-user client as a necessary requirement at contract-signing times, and words provided in contracts. But the end users quite often do not use the tools that are provided; security is taken for granted, and the tools are not used as adequately as they could be. Certainly there are a number of services available from hardware vendors and software service companies, and the costs are not significant at all.

[Traduction]

chapitre intitulé «Mémoire de *Datacrown* adressé à la Consultation nationale sur les infractions relatives aux ordinateurs».

M. Kay: Nous avons joint ce document aux fins de consultation complémentaire, pour le cas où nous aurions à . . . Mais dans ses grandes lignes, il ne fait que résumer ce que contient notre mémoire écrit.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Je vais maintenant donner la parole au premier intervenant, qui sera M. Boire.

Monsieur Boire, je remarque à la première page de vos notes que d'après vous les sociétés membres couvrent presque tous les aspects de l'informatique. Plus loin, vous parlez de la sécurité qu'offre votre organisme. Quelle sécurité est offerte par ceux qui fabriquent le matériel?

M. Boire: Notre association compte les plus gros fabricants de matériel; des gens comme *Control Data*, *Digital*, *IBM*. Si je ne m'abuse, vous avez reçu il y a quelque temps M. John Dean d'IBM; il a parlé des dispositions sécuritaires prises pour leurs clients. Evidemment, le fait que l'on offre certaines dispositions ne veut pas dire que le client s'en servira. C'est certain. Nous pouvons imposer un certain nombre de conditions au client, lui donner certains renseignements, mais il est bien sûr difficile d'appliquer cela ou de savoir si les conditions sont respectées.

Bien des difficultés proviennent vraisemblablement de la faiblesse ou de la négligence humaine. Les gens sont souvent négligents dans l'utilisation de leurs terminaux. Ils les laissent branchés ou écrivent leur mot de passe et le laisse à la disposition de tout le monde. Il y a des tas de moyens d'anéantir les bienfaits d'un système si l'utilisateur se montre négligent.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous parlez de la difficulté d'appliquer les dispositions sécuritaires qui sont offertes, mais qu'en coûte-t-il? Est-ce important?

M. Boire: Je préférerais que Dwayne réponde, car il dirige la direction générale d'Ottawa d'une grande société utilisant ces systèmes.

M. Kay: Les dispositions sécuritaires, qu'il s'agisse du matériel ou du logiciel, sont tout à fait suffisantes aujourd'hui. On s'aperçoit en général que la sécurité est considérée comme très nécessaire par le dernier utilisateur lorsque l'on signe des contrats qui en font mention. Toutefois, il arrive très souvent que les derniers utilisateurs n'ont pas recours aux outils à leur disposition; on considère la sécurité comme acquise et l'on néglige les outils fournis. Les vendeurs de matériel offrent certes des services tout comme les vendeurs de logiciels, et les coûts ne sont pas élevés du tout.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): The costs are not significant?

Mr. Kay: No.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So it is a question, really, of trying to condition your members to use the security provisions that are made available.

Mr. Kay: Not so much the members, as a matter of fact; I think you would normally find that most service companies do provide the services. The onus is, in fact, upon the clients to avail themselves of the services that are there. As you say, it is more a question of the end-user client, an individual like yourself or myself, sitting on a console using a computer terminal and disciplining ourselves to using passwords and protecting passwords, as you would your credit card for Sears or Texaco, that sort of thing, the numbers.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Kay, to what extent do you try to market the security provisions, or insist on the security provisions being accepted by the end user?

Mr. Kay: From a service company aspect, our particular company puts a good deal of stress on security in both our proposals and in the day-to-day consultation with clients.

• 1030

We encourage clients to make use of the security provisions and techniques that we provide, as a matter of course. Interestingly enough, while some clients are particularly good at availing themselves of those services, others treat them with a much less important role.

Mr. Boire: If I may, Mr. Chairman . . .

The Chairman: Yes.

Mr. Boire: —I would just like to say that there has been some discussion in the previous testimony about the fact that a lot of students in colleges and universities are often guilty of breaking into systems and hacking around with them. But I think at least one professor locally has a solution to that. The way he gets around it is he says if five identical solutions to the problem are submitted, both the creator and the plagiarizers will suffer, because he will divide the 100% amongst the five identical solutions submitted. So each person will only get 20%.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): In other words, what you are suggesting is if there is a conspiracy in doing this, they will all pay, and pay very heavily; even more than one would.

Mr. Boire: I thought that was a good way of discouraging that sort of plagiarism amongst the students.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Tell me, Mr. Boire, to what extent are we behind Europe and the United States and Japan in our security as far as the computer system is concerned?

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Non?

M. Kay: Non.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il s'agit donc, en fait, d'essayer de convaincre vos membres d'utiliser les dispositions sécuritaires offertes.

M. Kay: Pas tellement nos membres, car la plupart des sociétés de services offrent ces services. La responsabilité retombe en fait sur les clients qui doivent se prévaloir des services qui existent. Vous avez raison de dire que c'est plus le fait du client, de l'utilisateur, de quelqu'un comme vous et moi qui se trouve devant une console et utilise un terminal. Il s'agit de savoir utiliser et protéger les mots de passe comme on fait attention à protéger les numéros d'une carte de crédit Sears ou Texaco.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Kay, dans quelle mesure essayez-vous de commercialiser les dispositifs sécuritaires ou d'insister pour que les utilisateurs appliquent les dispositions sécuritaires?

M. Kay: Du point de vue d'une société de services, nous insistons beaucoup sur la sécurité à la fois dans nos propositions et dans les consultations régulières que nous avons avec les clients.

Nous encourageons les clients à utiliser les dispositions et techniques sécuritaires que nous offrons, c'est évident. Ce qui est intéressant, c'est que si certains clients sont tout à fait prêts à se procurer ces services, d'autres les jugent beaucoup moins importants.

M. Boire: Monsieur le président, si vous me permettez . . .

Le président: Certainement.

M. Boire: . . . je voulais simplement dire que l'on a un peu discuté du fait que beaucoup d'étudiants, dans les collèges et universités, sont souvent coupables, car ils entrent en tiers dans un système qu'ils s'amusent à utiliser. Je crois qu'au moins un professeur a trouvé une solution. Il dit en effet que si l'on soumet cinq solutions identiques au problème, le créateur et les plagiaires en souffriront, car il divisera en cinq la note qu'il aurait donnée à la solution. Chacun n'obtient donc que 20 p. 100 de la note.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous suggérez donc que s'il y a conspiration, tout le monde paie et paie très cher; même plus que normalement.

M. Boire: Je pensais que c'était une bonne idée pour éviter ce genre de choses chez les étudiants.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Boire, dans quelle mesure sommes-nous en retard sur l'Europe, les États-Unis et le Japon en matière de sécurité informatique?

[Texte]

Mr. Boire: Well, as I mentioned earlier, we have an association with the European Computer Services Association, ECSA.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): But most of these countries have legislation already on the books, have they not?

Mr. Boire: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Is Canada the only country that does not have any legislation on the books, of the countries that are users?

Mr. Boire: I know there is legislation in Europe, and there is some in a number of states in the United States. I think there are possibly 16 or 17 states that have some form of legislation now. I have a reference to some information, but I do not have detailed knowledge of it, about the situation in Japan. I received it very recently. It was just a flyer that came in the mail on software protection in Japan. This is a study that has been done. It talks about Japanese copyright, the protection of software, protection of works in Japan, protection of works created by a national corporation non-member. It provides a great deal of detail on this. I have not read it. I just received this in the mail. I am not aware of what the situation is currently in Japan.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Boire, I think you said your members do not see the computer situation as a critical issue at the present time, and they are not really getting excited about it, even though we have nothing on the statute books that really covers it, from the point of view of Criminal Code protection or in coverage by other pieces of legislation, either provincial or federal. Is this still your opinion?

Mr. Boire: That is the impression that I get. From the association headquarters here we have sent out information about what is going on. We have solicited input from our members in connection with the national consultation put on by the Department of Justice in Toronto in co-operation with CIPS; and of course many of the people in our companies, the practitioners of the art or science, are members of CIPS, and many people in our companies have participated in that way, through individuals. But the only company that provided input on that occasion was Datacrown. Other companies have expressed a, shall I say, medium-priority interest in it. A few have said they had a low-priority interest in it. But I cannot really say, other than Datacrown, who have put in their submission, that any other company has come back and said this was really a critical issue.

• 1035

I tend to think that this is not because people are not concerned about it but that maybe they are more concerned in the immediate future with things like taxation on software and the research and development allowances for the development of software and that sort of thing, which they consider, maybe, at the moment more vital to their interests.

I think maybe it is like insurance: after you have a fire, you suddenly wish you had more.

[Traduction]

M. Boire: Comme je le disais tout à l'heure, nous sommes associés à l'Association des services informatiques européens.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais la plupart de ces pays ont déjà des lois à ce sujet, n'est-ce pas?

M. Boire: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Le Canada est-il le seul pays utilisateur d'information à n'avoir pas légiféré en la matière?

M. Boire: Je sais qu'il y a des lois en Europe et dans un certain nombre d'États aux États-Unis. Seize ou dix-sept États, si je ne m'abuse. Je n'ai pas le détail quant à la situation au Japon. J'ai reçu une documentation très récemment, un prospectus qui est arrivé par le courrier sur la protection du logiciel au Japon. C'est une étude qui a été effectuée. Il s'agit des droits d'auteur japonais, de la protection du logiciel, de la protection des travaux au Japon; de la protection des travaux réalisés par une société nationale non membre. Le prospectus contient beaucoup de détails, mais je ne l'ai pas lu, car je viens de le recevoir. Je ne sais donc pas ce qu'il en est exactement au Japon.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Boire, je crois que vous avez dit que vos membres ne jugeaient pas que le problème de l'informatique était extrêmement grave à l'heure actuelle et que cela ne les inquiète pas tellement, bien que nous n'ayons rien dans nos statuts pour couvrir de telles situations. Il n'y a rien à ce sujet dans le Code criminel ni dans d'autres lois provinciales ou fédérales. Avez-vous changé d'avis?

M. Boire: Non, c'est l'impression que j'ai. Nous avons envoyé de notre siège social ici des renseignements sur ce que l'on faisait, nous avons demandé à nos membres de donner leur avis sur la consultation nationale entreprise par le ministère de la Justice à Toronto en collaboration avec la CIPS; et il y en a évidemment beaucoup dans nos sociétés, ceux qui pratiquent l'art ou la science, qui sont aussi membres de la CIPS et qui ont par là participé à cette étude. La seule société qui l'ait fait à titre de société était Datacrown. D'autres sociétés ne s'y sont intéressées qu'à moitié. Certaines ont même dit que cela ne les intéressait pas vraiment. Je ne puis donc vraiment dire, sauf pour Datacrown qui a présenté un mémoire, que d'autres sociétés aient vraiment déclaré que c'était un problème critique.

Je pense que ce n'est pas parce que les gens ne s'en inquiètent pas, mais peut-être parce qu'ils s'inquiètent plus dans l'immédiat de choses comme l'imposition du logiciel et les allocations à la recherche et au développement qui pour le moment touchent leurs intérêts de plus près.

C'est peut-être comme l'assurance: après un incendie, vous regrettez de ne pas avoir été mieux assuré.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Would it be fair to say that if they are not concerned maybe it is because they are not aware? I am wondering what your organization is doing to make them more aware.

Mr. Boire: Following the consultation in Toronto we invited some of the people who participated in that, along with myself, to make a presentation at our chapter meeting in Toronto on April 20. We have about, I guess, 30 member companies in Toronto, and 17 came out for that presentation. So we have tried to awaken or reawaken their interest in the subject and make them aware of what is going on.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have come out with a code of ethics, which is something I was looking for. Do you see this code of ethics as you have it today as something that your members should be using to self-regulate, or do you see that it might be incorporated in some way in a piece of legislation?

Mr. Boire: I would think our members would prefer to have this a self-legislated thing rather than to see a code of ethics incorporated into legislation.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Now you are talking, really, about your members, but what about the non-members? How do you see them being controlled by any code of ethics or being even concerned about a code of ethics?

Mr. Boire: There are of course many, many companies that are not members of our association. I guess in terms of the dollar volume of processing in Canada our association represents close to 50% of all the data processing that is done in Canada, even though our membership is 70 companies out of . . . There may be 1,000 companies in the field, but as in most industries a relatively small number of companies tends to do a large proportion of the business.

It is a difficult point that is a good question. One way, of course, we would like to solve that problem would be to have those other 900 companies join our association.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I am just wondering what we should be thinking up in terms of not only having members such as you speak of complying with a standard code of ethics but having the non-members as well. Maybe they have another organization—this I do not know—but it would seem to me you are either in or you are out and if they are not in the organization then they are free to have any code of ethics they like and it is not playing according to what I would call the rules of the game. We should all be playing by the same rules. Whether this can be looked at through the eyes of the professionals in the field and organizations such as you represent or whether it should be placed in a statute in some way I sort of leave up to you to advise us.

Mr. Boire: I am not aware that there are codes of ethics, if you will, legislated in respect of other industries. Perhaps there are, but I am not aware.

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Peut-on alors dire que s'ils ne se préoccupent pas de la question, c'est peut-être parce qu'ils n'y sont pas sensibles? Que fait votre association pour les mettre au courant?

M. Boire: À la suite de la consultation à Toronto, nous avons invité certains participants à collaborer avec moi à la préparation d'un rapport pour la réunion d'un chapitre à Toronto le 20 avril. Je crois que nous avons environ 30 sociétés membres à Toronto et que 17 sont venues. Nous avons donc essayé d'éveiller ou de réveiller leur intérêt pour ce sujet et de les mettre au courant de ce que l'on faisait dans ce sens.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez produit un code d'éthique et c'est justement ce que je souhaitais. Pensez-vous que le code d'éthique que vous avez aujourd'hui puisse être utilisé par vos membres qui s'autodisciplineraient ainsi ou pensez-vous qu'il serait mieux de l'incorporer en quelque sorte à une loi?

M. Boire: Je pense que nos membres préféreraient s'autodiscipliner plutôt que de voir un code d'éthique incorporé à une loi.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous parlez-là en fait de vos membres, mais qu'en serait-il pour les autres? Comment pensez-vous qu'ils puissent être contrôlés et même s'inquiéter d'un code d'éthique?

M. Boire: Il y a évidemment des tas de sociétés qui ne sont pas membres de notre association. Je dirais qu'elles représentent toutefois près de 50 p. 100 de tout le volume d'information traitée au Canada, même si nous ne comptons que 70 sociétés sur . . . il y en a peut-être 1,000 dans ce domaine, mais comme dans la plupart des industries, ce n'est qu'un petit nombre de sociétés qui ont en général la part du lion du marché.

C'est une bonne question. Une façon pour nous de résoudre ce problème serait que les 900 autres sociétés adhèrent à notre association.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je me demande simplement ce à quoi il nous faudrait réfléchir pour que les autres sociétés se conforment à un code d'éthique standard. Peut-être ont-elles une autre association, je n'en sais rien, mais il me semble que si ces sociétés n'appartiennent pas à votre association, elles ne sont pas tenues de suivre votre code d'éthique si bien qu'elles ne suivent pas ce que j'appellerais les règles du jeu. Nous devons tous adopter les mêmes règles. C'est pourquoi je vous demande s'il faut envisager cela par l'intermédiaire de professionnels et d'organismes comme le vôtre ou au contraire, envisager de légiférer.

M. Boire: J'ignore s'il y a des codes d'éthique contenus dans des lois pour d'autres industries.

[Texte]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): One of the things you seem to be quite concerned about—and we are to—is the whole question of definition. You mentioned Gotlieb, who has a number of definitions; you have indicated some definitions yourself. It seems to me it is something like Alice in Wonderland. She was asked by the Mad Hatter, I think it was: Why do you not say what you mean? She said: Well, I mean what I say; it is the same thing, is it not? I do not know whether it is.

What seems to be happening is that, like in *Alice in Wonderland* or *Through the Looking-Glass*, one of the two, she says when she uses a word it means what she says it means, nothing more and nothing less, and what you are doing here is giving a new definition to some of the words that have maybe a lesser definition than you are giving to them. Do you find that this list that you have given so far is a finite list, or are there many, many others that should be given an extended definition?

• 1040

Mr. Boire: I think your example is rather an apt one, because many people today probably feel a little bit like Alice in Wonderland when they look around them and see the kind of explosion that is going on in the computer field. All the new developments and the new technology tends to become a little bewildering to a lot of people, particularly people who have not, say, grown up with it. I think the youngsters in school today are not having any difficulty at all. They are learning it at school and they take to it very readily and very easily.

But what you have quoted is very true. When I use a word, it means exactly what I say it means, and I think this is probably true—and although I am not a lawyer, I think this is true in a legal sense—that in a contract the term has the meaning that is defined in the contract. That may not be the generally acknowledged or public understanding of the word, but this is the legal understanding of it. I think it is important that there be such definitions in the law, although I recognize the great difficulty in arriving at acceptable definitions.

I recall that at the consultation in Toronto there were, I believe, 35 people from all across Canada—people from associations like our own, people from universities, people from companies—and they were all “experts”, and yet probably the only thing the experts could agree upon from the draft definition that had been provided to them for discussion was that they did not like it. I guess a number of people came up with alternative definitions, but it was difficult amongst a group of 35 people to come up with a definition that everybody could accept.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you, Mr. Boire.

We are just going to adjourn this meeting for a couple of minutes while the main committee takes over, and then we will be right back again with more questioning.

[Traduction]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il y a une chose qui semble beaucoup vous préoccuper, et nous aussi d'ailleurs, c'est toute la question des définitions. Vous dites que M. Gotlieb a plusieurs définitions; vous avez vous-même donné certaines définitions. Il me semble que c'est un peu Alice au pays des merveilles. On lui avait demandé: Pourquoi ne dites-vous pas ce que vous voulez? Elle répondit: Parce que je veux dire ce que je dis; c'est la même chose, non? Je ne sais pas.

Comme dans «Alice au pays des merveilles» ou je ne sais plus dans quel épisode, elle dit que lorsqu'elle utilise un mot, il signifie ce qu'elle dit qu'il signifie, rien de plus et rien de moins, et là vous donnez une nouvelle définition de certains des termes qui ne satisfont peut-être pas exactement la définition que vous donnez. Pensez-vous que cette liste que vous avez donnée est complète ou il y en a-t-il beaucoup d'autres auxquelles il faudrait donner des définitions élargies?

M. Boire: Je crois que vous avez donné un bon exemple car beaucoup de gens ont probablement un peu le sentiment d'Alice lorsqu'ils découvrent l'explosion du secteur informatique. Toutes les nouvelles découvertes et la technologie nouvelle effraient beaucoup de gens, surtout ceux qui ne suivent pas cette évolution de près. Les jeunes écoliers d'aujourd'hui n'ont pas peur du tout. Ils apprennent cela à l'école et ils s'y mettent très volontiers et très facilement.

Mais vous avez tout à fait raison. Lorsque j'utilise un terme, il signifie exactement ce que je dis qu'il signifie et je crois que c'est probablement vrai—bien que je ne sois pas avocat, je crois que c'est vrai au sens légal—que dans un contrat, le terme a le sens défini dans le contrat. Ce n'est peut-être pas toujours le sens généralement admis dans un contexte ordinaire, mais c'est son interprétation juridique. Je crois qu'il est important d'avoir de telles définitions dans la loi même si je reconnais qu'il est extrêmement difficile d'en trouver d'acceptables.

Je me souviens qu'à Toronto, il y avait quelque 35 personnes venues de tous les coins du pays—des gens appartenant à des associations comme la nôtre, des gens représentant des universités ou d'autres sociétés—tous des «experts» et la seule chose sur laquelle les experts ont réussi à se mettre d'accord à propos du projet de définition qui avait été soumis, c'est que la définition ne leur plaisait pas. Certains ont proposé d'autres définitions mais il était difficile pour un groupe de 35 personnes de parvenir à une définition qui plaise à tous.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci, monsieur Boire.

Nous allons ajourner la réunion pour deux minutes pour permettre au comité principal de s'installer. Nous reprendrons les questions immédiatement après.

[Text]

• 1043

[Translation]

• 1045

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): We are back in business again. Mr. Boire, I will ask you a few more questions and then we will turn to Mr. Beatty.

One of the difficulties I see is that you have a number of words that you wish to define, and in defining the words you tend to define them in other words that require definition as well. This just tends to complicate the situation even more. For instance, you talk about the term "licensed program", which you say:

shall mean a licensed information processing program, or programs consisting of a series of instructions or statements which is machine readable.

I think the term "machine readable" really needs to be explained also, and maybe in explaining that you would come up with other words that have to be explained.

Mr. Boire: Yes, I recognize the difficulty there. Each industry, trade or profession has a kind of jargon that grows up around it, which is meaningful to the people in the industry but tends to be meaningless to people outside of it.

I think the words "machine readable" are probably good ones in the sense that they do not say "electronically readable" or "optically readable". It is a very broad term. Back in the days when I first became involved with computers... Back in 1949, probably the first computer that was ever built in Canada was built by Computing Devices on a contract from the navy for a tactical trainer. My company, Measurement Engineering Limited, at the time had a contract for the display devices for this computer. At that time, I suppose the total market for computers in North America was maybe six, so it was not exactly a thriving field then. But when you talk about machine readable, the machine that Computing Devices was developing then consisted of something like 10,000 vacuum tubes and maybe 5,000 electromechanical relays. The memory was an electromechanical relay-type memory.

Of course, there have been all kinds of changes, technologically, since then, and you do not find very many, if any, relays in computers today. So if the definition were to say that the information should be readable in terms of the position of electro-mechanical relays, or in terms of electrical impulses, or even in terms of optical signals that tie it to the current technology, it might very rapidly become obsolete, because, as I mentioned earlier, even today people are working biologically with microbes and things that can be programmed to exhibit certain characteristics, and predictions are that in the not too distant future there may be a form of computer that consists of colonies of microbes that do things with data.

"Machine readable" maybe has the difficulty that it talks about "machine", and maybe the machine will be a bunch of microbes, and I do not know whether that would be legally acceptable, to consider microbes as machines.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Nous reprenons. Monsieur Boire, j'aurais quelques autres questions à vous poser et je passerai ensuite la parole à M. Beatty.

Une des difficultés est à mon avis que l'on souhaite définir un certain nombre de termes et qu'en les définissant, on a tendance à le faire en d'autres termes qu'il faudrait également définir. Cela tend donc à compliquer encore davantage la situation. Par exemple, vous parlez de «programme licencié», ce qui, dites-vous:

signifiera un programme de traitement de l'information licencié ou des programmes consistant en une série d'instructions ou de déclarations ordiolingues.

Je crois que l'expression «ordiolingues» doit vraiment aussi être expliquée et peut-être qu'en voulant l'expliquer vous utiliserez d'autres termes qu'il faudra aussi expliquer.

M. Boire: En effet, je reconnais la difficulté. Chaque industrie, métier ou profession a son jargon qui signifie bien quelque chose pour les spécialistes mais en général très peu pour les non spécialistes.

Je crois que le terme «ordiolingues» et probablement bien choisi en ce sens qu'il ne dit pas «lisibles électroniquement» ni «optiquement». C'est très vague. Lorsque j'ai commencé à m'intéresser aux ordinateurs... En 1949, le premier ordinateur qui avait été construit au Canada l'avait été par *Computing Devices* ayant reçu un contrat de la Marine pour un appareil tactique. Ma société, *Measurement Engineering Limited*, avait reçu un contrat pour l'unité d'affichage de cet ordinateur. Je suppose qu'alors le marché des ordinateurs en Amérique du Nord se limitait à six si bien que l'on ne pouvait encore parler d'un secteur en pleine expansion. Quand on parle de quelque chose qui est ordiolingue, la machine qu'avait alors conçue *Computing Devices* consistait en quelque 10,000 tubes vides et peut-être 5,000 relais électromécaniques. La mémoire était un système de relais électromécaniques.

Il est évident qu'il y a eu des tas de transformations et de progrès technologiques depuis et que l'on ne trouve pratiquement plus de relais dans les ordinateurs modernes. Si donc la définition était que l'information devait être lisible par relais électromécaniques ou par impulsions électriques ou encore par signaux optiques, elle risquerait de devenir très rapidement désuète car, comme je l'ai dit tout à l'heure, même aujourd'hui on travaille en biologie avec des microbes et des choses que l'on peut programmer pour montrer certaines caractéristiques et l'on peut s'attendre à ce que dans un avenir pas très éloigné il y ait une génération d'ordinateurs qui consiste en une colonie de microbes capables d'agir avec certaines données.

Peut-être que l'expression «lisible à la machine», ou «ordiolingue», vous gêne parce qu'il est question de «machine» et peut-être que cette machine sera un jour un ensemble de

[Texte]

These are some of the difficulties inherent in trying to define a thing now in terms that will be acceptable and useable maybe 10 years from now.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Is it fair to suggest that the jargon that you have adopted, and your members have obviously adopted, applies also to non-members and to users?

Mr. Boire: I would think these terms are very widely used within the industry.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You mentioned in your notes, under security, something to do with a built-in bug—in the programming, I assume—so that if someone is trying to access the information it will either self-destruct, or something will happen to it. Would you just explain that a little bit further? Is this one of your basic security measures that you advise the users to adopt?

Mr. Boire: It is a measure that is used by some people.

• 1050

In fact, I just received a letter from one of our members in which he mentioned that. This is a small company that has done some software development and, as I mentioned earlier, this is a very expensive process which is one of the factors which inhibits people to a degree; the people who do programming are scarce. As a result, their salaries are high and it is difficult for a small company to get involved in this to a large degree, so that when they do they try to build in safeguards within the programming.

When the programmer writes a program in a programming language—and there are many of these languages now and they are developing and proliferating . . . because of the high cost of the programmers' services more people are using what are called "high level languages", languages like Pascal or ADA where the programmer can make the computer do a lot of things by just writing one line of code instead of in the early days where he had to program the machine in terms of binary code where every single action in the machine had to be spelled out in zeros and ones.

When the programmers write these source codes they will often put some instructions in the code that, as I said, will cause it to self-destruct or to give an indication if somebody is tampering with it at the machine end. Within the computer, the interpreter or compiler takes the source code and turns it into an object code that is machine readable. This machine code, to a human being, means nothing, but the machine can read it, and this bug can be planted in there by the writer of the program. Of course, each programmer will have his own approach to it. Some are more sophisticated than others, and these languages, of course, are becoming more and more sophisticated. It is difficult to keep up with all the developments.

[Traduction]

microbes et qu'alors je ne sais pas s'il sera légalement acceptable de considérer les microbes comme des machines.

Ce sont les difficultés inhérentes à la définition de termes actuels qui ne pourront peut-être plus s'appliquer dans dix ans.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Peut-on alors dire que le jargon que vous avez adopté et que vos membres ont de toute évidence adopté s'applique aussi à ceux qui ne sont pas membres de votre association et aux utilisateurs d'ordinateurs?

M. Boire: Je pense que ces termes sont en effet largement utilisés dans l'industrie.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À propos de sécurité, vous avez mentionné dans vos notes quelque chose sur un défaut de programmation intégrée, si je ne m'abuse, qui fait que si quelqu'un essaie d'accéder à l'information, quelque chose se produit ou l'information disparaît. Pourriez-vous expliquer un peu mieux la chose? Est-ce une des mesures élémentaires de sécurité que vous engagez vos membres à adopter?

M. Boire: C'est une mesure qu'utilisent certains.

En fait, je viens de recevoir une lettre d'un de nos membres qui parle justement de cela. Il s'agit d'une petite société qui a fait un peu de conception de programme et, comme je le mentionnais tout à l'heure, le coût est tellement élevé que rares sont ceux qui font de la programmation. Ainsi les salaires sont-ils élevés et est-il difficile pour une petite société de se lancer là-dedans à grande échelle si bien que lorsqu'elle le fait elle essaie d'intégrer certaines garanties au programme.

Lorsque le programmeur écrit un programme dans un langage informatique—et il y a maintenant beaucoup de langages—étant donné le coût élevé de ces services, les utilisateurs de ce qu'on appelle les «langages de haut de gamme» comme le Pascal ou l'ADA sont plus nombreux car le programmeur peut faire faire à l'ordinateur énormément de chose en se contentant d'écrire une ligne de code plutôt que comme on le faisait autrefois de programmer la machine en binaire où toute opération devait être exprimée sous forme de zéros et de uns.

Lorsque les programmeurs écrivent ces codes d'origine ils mettent souvent des instructions dans le code qui feront qu'il se détruira de lui-même ou qu'il signalera si quelqu'un essaie de l'utiliser illégalement. Dans l'ordinateur, l'interprète ou le compilateur prend le code d'origine et le transforme en code compilé exploitable sur machine. Ce code machine ne signifie rien à un être humain mais la machine peut l'exploiter et cette défaillance peut être implantée là par l'auteur du programme. Il est évident que chaque programmeur a sa propre méthode. Certaines sont plus complexes que d'autres et ces langages deviennent bien sûr de plus en plus complexes. Il est difficile de suivre toutes les nouveautés.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Boire, our time is really short and I have about three short questions to which I would like to get three short answers if possible, and then turn it over to Mr. Beatty who has not had an opportunity to question you.

Mr. Beatty: Mr. Chairman, I apologize that I have been in and out because of other business.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): On page 9 of your statement, you set out a number of criteria for employees to be involved in this kind of employment. I am wondering if any of these, in your view, offend any human rights legislation?

Mr. Boire: I might mention that these come from a government request for proposals, and these are the requirements that are imposed upon the bidders. The successful bidder must do these things. I guess I would have to beg off answering whether this contravenes any of the human rights legislation. I am not a lawyer and I am not necessarily completely up to date on that.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): On page 10, you talk about definition of theft in the Criminal Code, and particularly you refer to tangible property. Would it not be helpful if the definition were tangible or intangible?

Mr. Boire: This is something that a lot of people have argued about, I guess, for a long time. I think there are difficulties both ways. I think some people are concerned that if data and information is defined as tangible property that this may involve more than is bargained for, in terms of the end result.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You think the word intangible is too broad in its connotation?

Mr. Boire: You see, it depends again on your background and your training, how you understand that. To me, electrical impulses are quite tangible, because I am an electronic engineer by profession and all my life I have been able to measure and to see on oscilloscopes and to read on meters electrical impulses. To me they are quite tangible, but the legal definition of tangible, I guess, is something else—it goes back a long time, before electronics existed.

• 1055

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You made a statement that data can now be transported or transmitted outside of Canada, and used in a totally uncontrollable manner. The words uncontrollable manner I find rather difficult to accept. Are you suggesting that it is absolutely infinite, that there is no way that there can be any control at all?

Mr. Boire: I was thinking more, I guess, in terms of personal information that individuals—information in government data banks, shall we say, that probably Canadians believe should be

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Boire, nous n'avons pas beaucoup de temps et j'aimerais encore vous poser trois questions en vitesse en espérant que vous pourrez également y répondre brièvement avant que je ne cède la parole à M. Beatty qui n'a pas encore pu vous interroger.

M. Beatty: Monsieur le président, je suis désolé d'avoir dû m'absenter mais j'avais d'autres obligations.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À la page 9 de votre déclaration, vous donnez un certain nombre de critères pour les employés de ce secteur. Certains d'entre eux seraient-ils à votre avis contraires à la Loi sur les droits de la personne?

M. Boire: Je dois dire que ceux-là ont été préparés à la demande du gouvernement et ce sont les conditions imposées aux soumissionnaires. Il faut s'y conformer si l'on veut obtenir un contrat. Je ne crois donc pas que je puisse vous dire si cela contrevient ou non à la Loi sur les droits de la personne. Je ne suis pas juriste et je ne suis peut-être pas tout à fait à jour là-dessus.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À la page 10, vous parlez de la définition de vol dans le Code criminel et en particulier de propriété tangible. Ne serait-il pas utile que la définition soit tangible ou intangible?

M. Boire: C'est quelque chose dont on discute beaucoup depuis longtemps. Je crois que cela pose des difficultés dans les deux cas. Certains s'inquiètent en effet que si les données et l'information sont considérées comme une propriété tangible, les résultats peuvent être plus forts que ce que l'on souhaitait.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous pensez que le terme intangible est trop vague dans ce sens?

M. Boire: Vous savez, tout dépend encore de votre milieu et de votre formation, de la façon dont on comprend les choses. Pour moi, les impulsions électriques sont tout à fait tangibles, car je suis ingénieur électronique de profession et que toute ma vie j'ai pu mesurer et voir ces impulsions électriques sur les oscilloscopes et autres appareils de mesure. Pour moi, c'est tout à fait tangible, mais la définition légale de tangible est autre chose, je suppose, cela remonte beaucoup plus loin que l'électronique.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez déclaré que l'on pouvait maintenant transporter ou transmettre des données à l'extérieur du pays et les utiliser sans aucun contrôle. Je trouve que l'expression «sans aucun contrôle» est assez difficilement acceptable. Est-ce vraiment sans aucun contrôle, n'y a-t-il aucune possibilité?

M. Boire: Je crois que je pensais plus aux renseignements personnels que les particuliers... les informations contenues dans les banques de données du gouvernement, par exemple,

[Texte]

kept private, or should be kept in Canada, and not be used by people outside of the country in an uncontrollable manner. The fact that you can shoot this up to a satellite and bounce it back almost anywhere in the world makes it possible for people to do that.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Just one further question for you, Mr. Boire. Would you comment on the guidelines from this government department that you appended to your statement today as Appendix B? Are they satisfactory, are they acceptable? Is there any problem with them? Do you recommend them?

Mr. Boire: I would like to pass that one to my colleague, Mr. Kay.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Kay, would you give us your opinion, please.

Mr. Kay: The guidelines and requirements of the Department of Supply and Services for successful bidders are guidelines and requirements which have evolved with the assistance of the industry, and there has been a fairly good rapport there. A cursory comment is, I do not believe, at this point, that we have as an industry any difficulty meeting them. As a matter of fact, there is a good deal of discussion on an ongoing basis with the Department of Supply and Services and normally, when a requirement comes up, industry is quite adept at moving to respond to the government requirement and if a problem arises, it is usually worked out reasonably well.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Beatty, do you wish to ask...? Well, then, I have a few more. I am not clear, Mr. Kay, from your dissertation, whether in fact you feel that the way to go is through, say, amending the 51 statutes or more federally that might have something to do with computers, or change the Criminal Code, or do both. Would you like to make some recommendations in that connection?

Mr. Kay: We believe quite firmly that the need to amend legislation is now because, as Mr. Boire indicated earlier, it is time to close the barn door before the horse gets out, and we think it will. We feel that the Criminal Code should and must be amended to adequately accommodate today's technology. But as indicated earlier, there is always a problem in getting a judge or jury's attention relative to these matters which are very impersonal, and more to the interest of the parties involved. So subsequently, we also think having the civil law changed would be most beneficial. Essentially, there is a need for both.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You mentioned a number of sections of the Criminal Code in particular that might be applicable. Did you take a look at the mischief's section, in particular?

Mr. Kay: I cannot comment on that, not being a lawyer, but we did have Mr. Pierre Boire, our corporate counsel—we did a fairly thorough review. There was some comment made relative to mischief, but I cannot recall what it was at this point.

[Traduction]

que les Canadiens voudraient probablement voir garder confidentielles ou gardées au Canada, ils ne voudraient pas que des étrangers les utilisent sans contrôle. Le fait que l'on puisse les envoyer par satellite et les diffuser pratiquement partout dans le monde rend la chose possible.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ma dernière question, monsieur Boire. Pourriez-vous donner votre avis sur les lignes directrices données par le gouvernement que vous avez jointes à votre déclaration sous le titre Annexe B? Vous semblent-elles satisfaisantes, acceptables? Posent-elles des problèmes? Les recommandez-vous?

M. Boire: Je préférerais que mon collègue, M. Kay, réponde.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Kay, voulez-vous nous donner votre avis, s'il vous plaît?

M. Kay: Les lignes directrices et les conditions imposées par le ministère des Approvisionnements et Services aux soumissionnaires ont été arrêtées en consultation avec l'industrie et je dois dire que cela s'est fait dans un bon esprit. Je ne pense pas que pour le moment l'industrie ait du mal à les suivre. D'ailleurs, on en discute toujours avec le Ministère et, normalement, lorsque le gouvernement demande quelque chose, l'industrie s'y soumet assez rapidement, et un éventuel problème est habituellement résolu de façon raisonnable.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Beatty, voulez-vous demander...? Non, alors j'aurais quelques autres questions. Je n'ai pas très bien compris, monsieur Kay, si vous estimez que le meilleur moyen serait de modifier les 51 lois ou plus qui, dans la législation fédérale, peuvent s'appliquer aux ordinateurs ou de modifier le Code criminel ou de faire les deux? Avez-vous des recommandations à ce sujet?

M. Kay: Nous croyons fermement qu'il est nécessaire de modifier la loi car, comme le disait tout à l'heure M. Boire, il est temps d'agir, sinon il sera trop tard. Nous estimons que le Code criminel doit être modifié en fonction de la technologie moderne. Comme nous le disions aussi, il y a toujours le problème d'attirer l'attention du juge ou du jury sur ces questions très impersonnelles qui intéressent plus les parties en cause. Nous pensons donc qu'il serait également utile de modifier le droit civil. Bref, que l'un et l'autre doivent être modifiés.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez signalé un certain nombre d'articles du Code criminel qui s'appliqueraient. Avez-vous envisagé l'article sur les dommages?

M. Kay: Je ne suis pas juriste, mais notre avocat, M. Pierre Boire, a examiné la question. On en a parlé en effet, mais je ne me souviens pas de ce qui avait alors été conclu.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): And do you feel that an amendment to Section 287 of the Criminal Code could be helpful? The bells are ringing, our time is up. We are going to have to adjourn.

• 1100

I want to thank both witnesses for appearing today, Mr. Boire and Mr. Kay. You have been more than helpful. You have given us a different perspective from what we have received already. I do hope you will keep in touch with the committee. I am sure you will. You will be reading the minutes, and if you have any further observations or any help that you can give the committee, we would be only too happy to receive it.

Our next meeting of the subcommittee will be on the same order of reference on Tuesday, May 24, at 11:00 a.m. in Room 208, West Block, with officials from the Department of Consumer and Corporate Affairs and officials from the Department of Communications.

The meeting is adjourned.

[Translation]

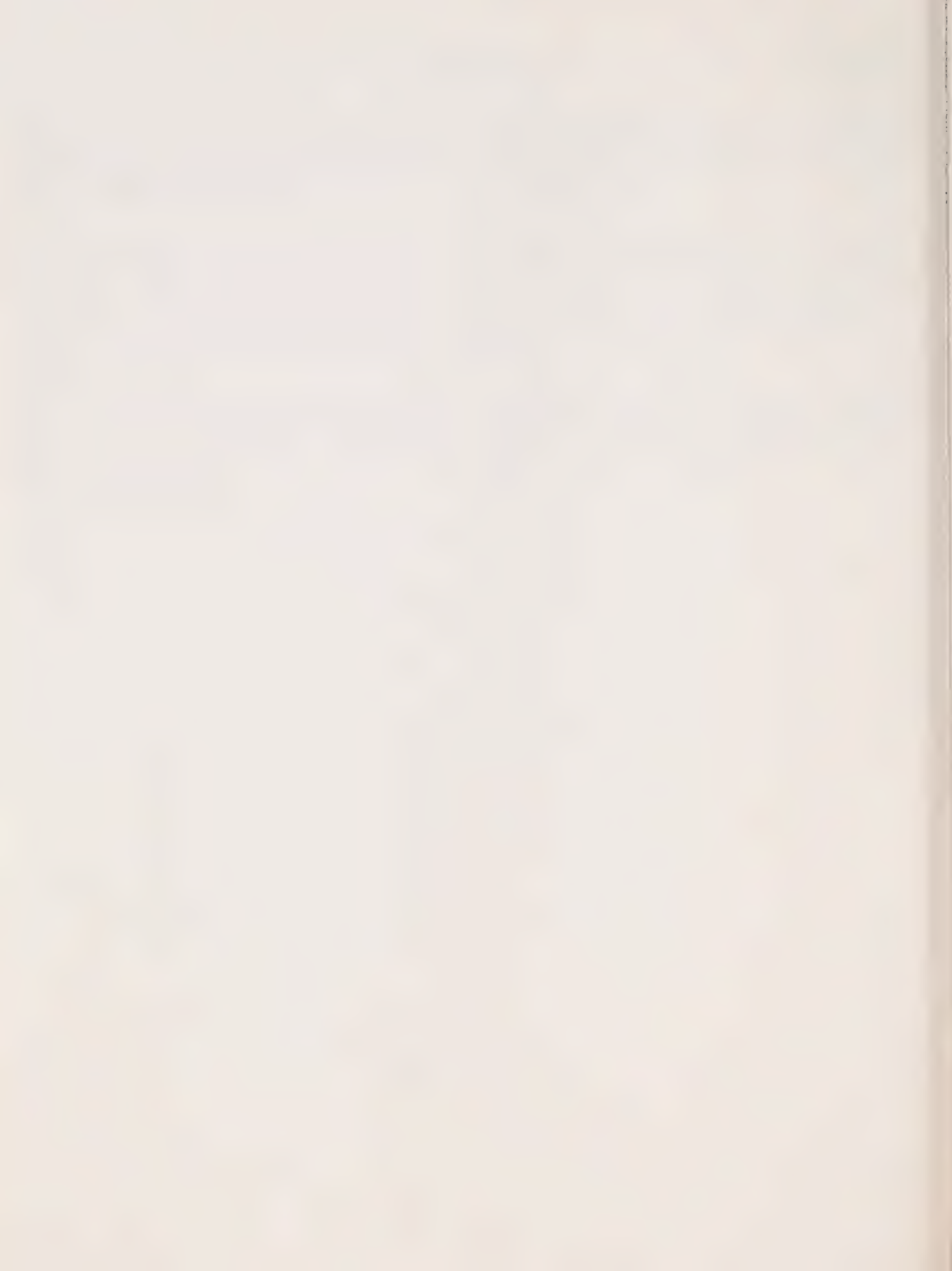
Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Et estimez-vous qu'un amendement à l'article 287 du Code criminel pourrait aider? La cloche sonne, c'est fini. Il nous faut ajourner.

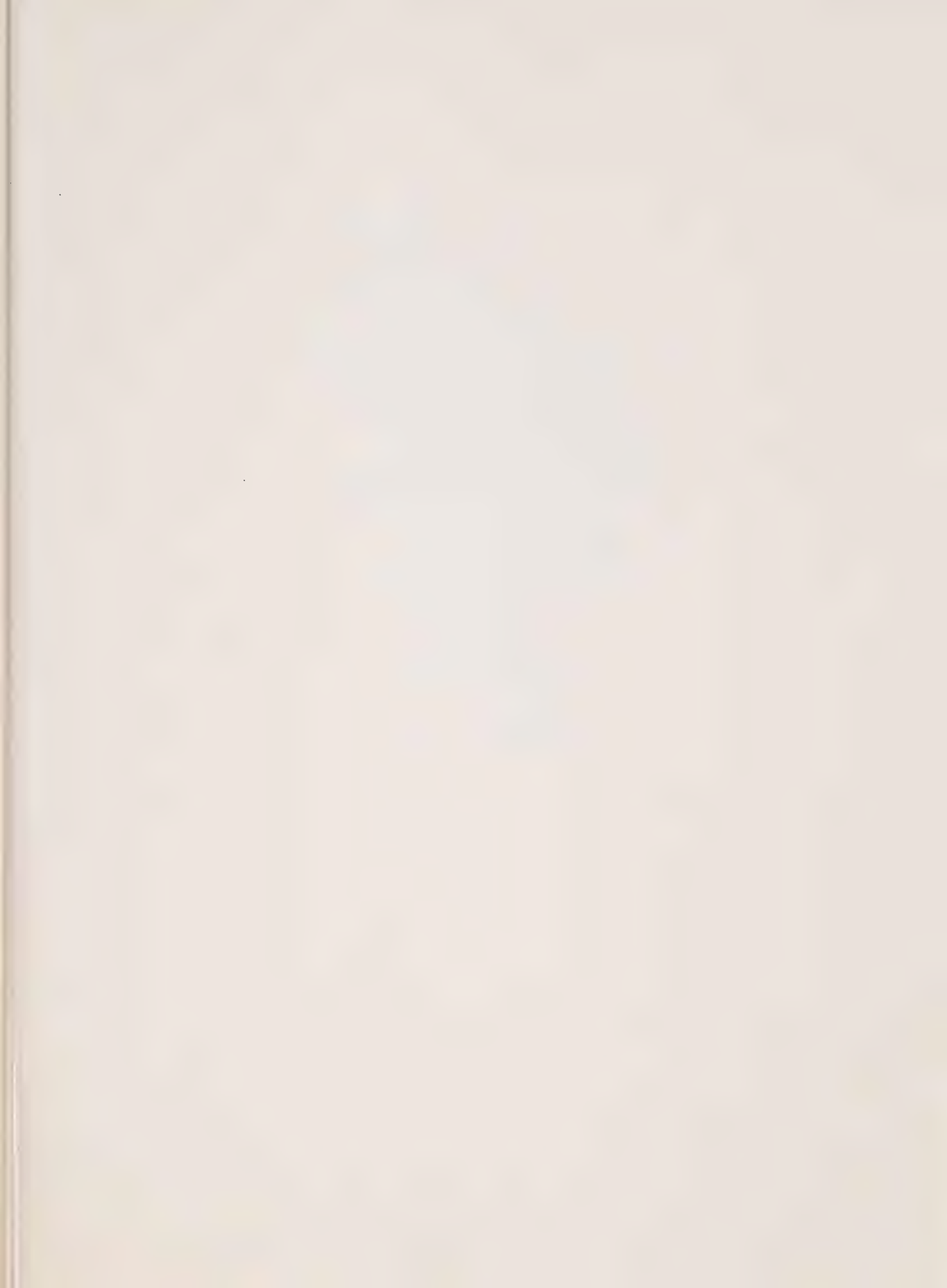
Je remercie les deux témoins, M. Boire et M. Kay, de toute l'aide qu'ils nous ont apportée. Vous nous avez donné des perspectives différentes. J'espère que vous resterez en contact avec le Comité. J'en suis d'ailleurs convaincu. Vous lirez le procès verbal et si vous voulez ajouter quelque chose ou nous soumettre vos recommandations, nous serons très heureux de les recevoir.

La prochaine réunion du Sous-comité portera sur le même ordre de renvoi et se tiendra le mardi 24 mai à 11h00, salle 208, Edifice de l'Ouest, alors que nous recevrons des fonctionnaires du ministère de la Consommation et des Corporations et du ministère des Communications.

La séance est levée.













*If undelivered, return COVER ONLY to
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9*

*En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9*

WITNESSES—TÉMOINS

Mr. Paul C. Boire Sr., President, Canadian Association of
Data Processing Service Organizations (CADAPSO),
Ottawa;

Mr. D.W. Kay, District Manager, Datacrown Inc., Ottawa.

M. Paul C. Boire Sr., Président, L'Association canadienne des
entreprises de services en informatiques (CADAPSO),
Ottawa;

M. D.W. Kay, Gérant de district, Datacrown Inc., Ottawa.

HOUSE OF COMMONS

Issue No. 11

Tuesday, May 24, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 11

Le mardi 24 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

TUESDAY, MAY 24, 1983

(13)

[Text]

The Sub-committee on computer crime met this day at 11:20 o'clock a.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Céline Hervieux-Payette.

Designated alternate Member present: Mr. Robinson (Etobicoke—Lakeshore).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From the Department of Consumer and Corporate Affairs: Mr. Tony Butler, Senior Policy advisor and Mr. Bruce Cauchman, Policy advisor.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (See *Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements and answered questions.

At 12:21 o'clock p.m. the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MARDI 24 MAI 1983

(13)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 11h 20, sous la présidence de M^{me} Céline Hervieux-Payette.

Membre du Sous-comité présent: M^{me} Céline Hervieux-Payette.

Membre substitut désigné présent: M. Robinson (Etobicoke—Lakeshore).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: Du Ministère de la consommation et des corporations: M. Tony Butler, Conseiller principal des politiques et M. Bruce Cauchman, Conseiller des politiques.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (Voir *procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations et répondent aux questions.

A 12h 21, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE*(Recorded by Electronic Apparatus)**[Texte]*

Tuesday, May 24, 1983

• 1121

Le président: À l'ordre!

Le Sous-comité reprend l'étude de son ordre de renvoi concernant les infractions relatives aux ordinateurs. Ce matin nous avons M. Tony Butler, conseiller principal des politiques et M. Bruce Couchman, conseiller des politiques du ministère de la Consommation et des Corporations. Vous êtes les bienvenus messieurs.

Je m'excuse d'être en retard. Je vous inviterais tout simplement à nous faire part de vos commentaires généraux et on pourra discuter ensuite de votre point de vue.

Je vous présente mon collègue M. Ken Robinson; M. Beatty, malheureusement ne sera pas ici ce matin. C'est un petit comité de trois personnes.

Monsieur Butler ou Monsieur Couchman, vous avez la parole.

Mr. Bruce Couchman (Policy Adviser, Department of Consumer and Corporate Affairs): Thank you, Madam Chairman. We have submitted a brief submission, which may provoke questions from you. I will basically outline the nature of our interest in this topic.

The Department of Consumer and Corporate Affairs is responsible for the intellectual property statutes, which are the Copyright Act, the Patent Act, the Industrial Design Act and the Trade Marks Act. We are concerned with property rights, or property protection, as they may attach to expressions of information or systems for manipulating information or, conceivably, even information itself. Our main interest, therefore, is in the nature of property rights as they might attach to expressions of information or systems for manipulating information. We simply wish to draw to the attention of the committee certain very fundamental principles of intellectual property protection which exist not only in Canada but in most, if not all, other countries of the world, and which are embodied in the major intellectual property treaties.

The two principles are, first, that not everything which is a product of the human mind or the human imagination receives intellectual property protection. Now, the basic principle, or the basic threshold, may vary depending on the type of protection which is desired. For example, the level necessary for patent protection is much higher than the level necessary for copyright protection. But to use the example of copyright protection, raw data or basic factual information is not itself protected by copyright. Once that data is given some special order or processed in some way, then it may in fact have copyright protection.

TÉMOIGNAGES*(Enregistrement électronique)**[Traduction]*

Le mardi 24 mai 1983

The Chairman: Order please.

The subcommittee resumes its study of the order of reference concerning computer related violations. We are honoured to have among us this morning, Mr. Tony Butler, Senior Advisor, policy analysis, and Mr. Bruce Couchman, Advisor, policy analysis, from Consumer and Corporate Affairs Canada; we wish to welcome them.

I regret being late. Please simply present your comments; we will discuss your opinion afterwards.

This is my colleague Mr. Ken Robinson. Unfortunately, Mr. Beatty will not be with us this morning. This will therefore be a small committee of three members.

Mr. Butler or Mr. Couchman, you have the floor.

M. Bruce Couchman (conseiller des politiques, ministère de la Consommation et des Corporations): Merci, madame le président. Nous avons présenté un bref mémoire qui peut-être soulever des questions. J'essayerai donc de décrire la nature de l'intérêt que l'on porte à ce sujet.

Consommation et Corporations Canada est responsable des lois qui touchent la propriété intellectuelle, c'est-à-dire la Loi sur le droit d'auteur, la Loi sur les brevets, la Loi sur les dessins industriels et la Loi sur les marques de commerce. Nous nous intéressons aux droits de propriété et à la protection de la propriété dans la mesure où ils concernent les modes d'expression de l'information, les systèmes de manipulation de l'information ou possiblement l'information elle-même. Par conséquent, nous nous intéressons principalement aux droits de propriété qui se rapportent aux modes d'expression et aux systèmes de manipulation de l'information. Nous aimerions simplement attirer l'attention du comité sur certains principes très fondamentaux de la protection de la propriété intellectuelle qui existent non seulement au Canada, mais dans la plupart sinon dans tous les autres pays du monde et qui font partie intégrante des principaux traités concernant la propriété intellectuelle.

Ces deux principes sont d'abord que tout produit de la pensée ou de l'imagination ne reçoit pas nécessairement une protection quant à la propriété intellectuelle. Il est évident que le concept de base ou le seuil peut varier selon le genre de protection voulue. Par exemple, le niveau de protection nécessaire pour les brevets est beaucoup plus élevé que le niveau de protection nécessaire pour les droits d'auteur. Si l'on prend l'exemple de la protection des droits d'auteur, les données brutes ou les renseignements factuels de base ne sont pas eux-mêmes protégés par les droits d'auteur. Une fois ces données placées selon un ordre quelconque ou traitées d'une certaine façon, elles peuvent obtenir alors la protection en vertu de la Loi sur le droit d'auteur.

[Texte]

With patent protection, a much higher standard is required before protection attaches. On the other hand, copyright protection is not an absolute form of protection. It is possible for another person independently to arrive at the same creation. It is only necessary for that person to show they did not copy the first created object.

This is particularly relevant perhaps with respect to computer programs, for it is quite possible that certain types of computer programs could be arrived at independently by two separate people; that is, there is a certain problem which people wish to resolve and people working quite independently could come up with basically the same solution. That particular aspect, or particular possibility, could create problems for the courts. So presumably that will be resolved in the future.

The second basic principle of intellectual property protection is that there is no form of intellectual property protection as such which is perpetual. Copyright protection provides the longest period of protection; that is, normally the life of the author plus 50 years. Patent protection is much shorter; that is, 17 years.

• 1125

The terms vary from country to country, but the term of copyright protection—the life of the author plus 50 years—seems to be the basic term that is accepted by most industrialized countries at the present time. It is the basic principle of copyright protection that at some point in time a person who owns an object or who has access to that object should be allowed to make copies of it. That is not only an essential aspect of copyright protection, but I think it is basically important for the functioning of the marketplace and the functioning of free competitive industrial growth.

We note that there are certain basic features of information expressed in computerized form which make it different from other sorts of objects or entities that are protected by intellectual property law. One is, with respect to copyright law, that computer programs, for example, may be embodied in a large number of objects which are sold to consumers and those consumers may not even be aware that that object contains a computer program. We think we must look very carefully, therefore, at extending traditional copyright protection in all its forms to computer programs, especially since, as I mentioned earlier, it is possible for people working independently to come up with basically the same program. The current Copyright Act contains provisions, for example, with respect to the importation of products or certain provisions with respect to deeming ownership and infringing copies which may not be appropriate for computer programs in machine-readable form.

[Traduction]

Dans le cas des brevets, il faut atteindre une norme beaucoup plus élevée avant d'obtenir la protection. D'autre part, la protection accordée en vertu des brevets n'est pas absolue. Il est toujours possible pour une autre personne d'arriver tout à fait indépendamment à produire la même création. Il est alors uniquement nécessaire pour cette personne de prouver qu'elle n'a pas copié le premier objet créé.

Ces principes sont particulièrement pertinents lorsqu'il s'agit des programmes informatiques car il est très possible que deux personnes différentes arrivent indépendamment à créer certains types de programmes informatiques; autrement dit, il existe un certain problème que les gens veulent résoudre et certaines personnes oeuvrant tout à fait indépendamment pourraient fort bien arriver à la même solution. Cet aspect particulier ou cette éventualité pourrait créer des problèmes pour les cours de justice. Nous supposons donc que cette difficulté sera réglée un jour.

Le deuxième principe de base quant à la protection de la propriété intellectuelle c'est qu'il n'existe aucune forme de protection de propriété intellectuelle qui est en soi permanente. La protection du droit d'auteur est celle qui couvre la plus longue période; elle dure habituellement pour la vie de l'auteur plus 50 ans. La protection des brevets dure beaucoup moins longtemps, c'est-à-dire 17 ans.

Les clauses varient de pays à pays, mais la durée de la protection du droit d'auteur, c'est-à-dire la vie de l'auteur plus 50 ans, semble être le terme accepté à l'heure actuelle par la plupart des pays industrialisés. Le principe même à la base de la protection du droit d'auteur veut qu'à un certain moment donné une personne qui possède un objet ou a accès à cet objet ait le droit d'en faire des copies. Il s'agit là d'un aspect essentiel de la protection du droit d'auteur, mais je crois qu'il s'agit aussi d'une idée fondamentalement importante pour le bon fonctionnement du marché et pour la croissance industrielle assurée par la libre concurrence.

Nous constatons qu'il existe certaines caractéristiques de base qui différencient les informations exprimées sous forme informatique des autres formes d'objets ou d'unités protégées par les lois sur la propriété intellectuelle. Une de ces caractéristiques, pour ce qui concerne la Loi sur le droit d'auteur, c'est que les programmes informatiques par exemple peuvent faire partie intégrante d'un grand nombre de produits différents vendus aux consommateurs et que ces consommateurs peuvent même ne pas savoir que le produit en cause renferme un programme informatique. Je crois, par conséquent, qu'il nous faut être très prudents lorsqu'on veut prolonger la protection traditionnelle du droit d'auteur sous toutes ses formes pour englober les programmes informatiques, étant donné surtout, comme je l'ai dit précédemment, qu'il est possible pour deux personnes travaillant indépendamment de créer sensiblement le même programme. La Loi sur le droit d'auteur courante renferme par exemple des dispositions se rapportant à l'importation de produits ou certaines dispositions se rapportant à la possession réputée du droit d'auteur et à la contrefaçon qui

[Text]

Although our major concern is with possible property rights in computerized information or expressions of information, we realize that other types of provisions . . . for example, dealing with access—may be quite relevant in terms of the functioning of the marketplace. For example, a law which restricted access to computer programs, if it covered objects which were lawfully in the possession of the consumer, could create problems in the functioning of the marketplace. For example, if I owned a computer game and the law on access prevented me, perpetually, from making a copy of that game, that access provision could, in effect, amount to the same as granting a property right in the computer game to the copyright owner which was of perpetual duration.

At the present time the status of information expressed in computerized form is unclear. It is a fairly basic principle of copyright law that is intended to protect information or expressions of information in the form which is intended for human comprehension or which can be readily comprehended by people. Thus the status of a computer program in the form of a micro-chip—that is, a form which can neither be correctly comprehended by the human senses nor which is intended to be comprehended by the human senses—is very unclear. We understand that certain cases are working their way through the courts as to whether information expressed in this form is currently protected by copyright law. Regardless of what the courts find—and this could be quite a lengthy process—it is the intention of the two departments involved in copyright law revision that the status of expressions of information embodied in a computerized form, whether that be data bases or computer programs, should be clarified in the Copyright Act so everyone should know the extent to which expressions of information in those two forms are in fact protected by copyright.

That is the gist of my remarks.

Thank you, Madam Chairman.

The Chairman: Mr. Butler, are you adding to this, or just willing to answer questions?

Mr. T. Butler (Senior Policy Adviser, Department of Consumer and Corporate Affairs): We are certainly willing to answer questions. I would just offer a very broad observation, and that is, first, it is the fundamental principle of copyright law that copyright protects the mode of expression. It does not protect the ideas or the information contained in the work. Now, one of the problems you have when you start dealing with complex technological machines, such as computers, is the loss, as a practical matter, of that distinction or reservation. For instance, when you buy a book, it is true the author has an exclusive right in the mode of expression, but you can use the book. You can lend it to your friends. You can read it.

[Translation]

pourraient n'être pas appropriées dans le cas des programmes informatiques sous forme assimilable par une machine.

Même si nous nous intéressons principalement aux droits éventuels de propriété de l'information informatisée ou des modes d'expression de cette information, nous réalisons que certains autres genres de clauses, par exemple les clauses se rapportant à l'accès, pourraient être très pertinentes quant au bon fonctionnement du marché. Par exemple une loi restreignant l'accès aux programmes informatiques, si elle touchait aussi les objets appartenant de droit à un consommateur, pourrait créer des problèmes sur le plan commercial. Si je possède un jeu d'ordinateur et qu'une partie de la loi m'empêche en permanence de faire une copie de ce jeu, cette clause concernant l'accès équivaut en fait à accorder un droit de propriété, quant à ce jeu d'ordinateur, au détenteur du droit d'auteur et ce, pour une durée indéfinie.

À l'heure actuelle, le statut de l'information exprimée sous forme informatisée n'est pas clair. Un des principes de base de la Loi sur le droit d'auteur c'est que celle-ci doit protéger l'information ou les modes d'expression de l'information présentés selon des formats que l'être humain peut comprendre ou saisir assez facilement. Par conséquent, le statut d'un programme informatique présenté sous forme de puce, c'est-à-dire selon un format que l'être humain ne peut ni comprendre ni proprement saisir et qui n'est même pas produit dans cette intention, est très incertain. Les cours de justice étudient à l'heure actuelle certaines causes qui visent à déterminer si pour le moment cette forme d'expression est protégée par la Loi sur le droit d'auteur. Peu importe la décision des cours, et les procédures pourraient durer longtemps, les deux ministères qui s'occupent de la refonte de la Loi sur le droit d'auteur veulent définitivement clarifier dans cette Loi le statut des modes informatiques d'expression de l'information, qu'il s'agisse de bases de données ou de programmes informatiques, pour que chacun sache dans quelle mesure l'information présentée selon ces deux formats est en fait protégée par la Loi sur le droit d'auteur.

Voilà en gros les points essentiels que je voulais présenter.

Merci, madame le président.

Le président: Monsieur Butler, désirez-vous ajouter des commentaires ou acceptez-vous simplement de répondre aux questions?

M. T. Butler (conseiller principal des politiques, ministère de la Consommation et des Corporations): J'accepterai avec plaisir de répondre aux questions, mais j'aimerais d'abord faire simplement une observation. Premièrement le principe fondamental de la Loi sur le droit d'auteur c'est que le droit d'auteur doit protéger le mode d'expression. Il ne protège pas les idées ou les renseignements contenus dans le travail. L'un des problèmes auxquels vous devez faire face lorsque vous traitez avec des appareils d'une technologie complexe comme les ordinateurs, c'est la perte, à toute fin pratique, de cette distinction ou de cette réserve. Par exemple, si vous achetez un livre il est vrai que l'auteur possède un droit exclusif quant à ce mode d'expression, mais vous pouvez utiliser le livre. Vous pouvez le prêter à des amis, vous pouvez le lire.

[Texte]

• 1130

To take an example of one of the Canadian decided cases, if you buy a cookbook, you can prepare meals and food according to the recipes in the book. As a practical matter, when you are dealing with machines, how do you separate the information so it is available to the public while at the same time preserving the rights of the author and the mode of expression?

Let me give you an example. It is a fairly mundane one. It is now possible to make fairly complex pieces of machinery, or automobile or other machinery parts, using machinery, machine tools, robots, constructed by computers. If a Canadian automobile parts supplier wants to make a replacement part for one of these parts and he subjects it to the conventional analysis to get the dimensions, that process is going to produce a computer data base and program which is going to look, for all practical intents and purposes, exactly like the one which was used by the original manufacturer of the automobile. As things presently stand, unless automobile parts are subject to patent protection, there is free competition in replacement parts.

I am giving that as an example of something which may strike you as being an unforeseen consequence of extending protection.

As Mr. Couchman has pointed out—and I think this is quite sound—if you are just operating on what I call the criminal law approach, forbidding unauthorized access, etc., then it is unlikely that you are going to get into these sorts of problems. I would emphasize this idea that non-protection, freedom of information, freedom of competition, free access to knowledge, are the general rule in our society. Restrictions on access are the exception. There is a danger, if one is too strict in dealing with access to information stored in computers, that we will go from the sort of society we have now to one which is a closed one. This is 1984 stuff, and I am not trying to create the horrors, but nonetheless it is something you have to be sensitive to, because as Bruce pointed out, the great difference between information in the form we are talking about now and the conventional means of storing information is that we cannot directly read it. Therefore you cannot “open up the book” and read the information and take it away.

We are open to questions, Madam Chairman. Mr. Couchman is an expert in copyright law. I do not pretend to be an expert there. My expertise is more in the area of patents and trademarks.

The Chairman: Would you say that the hardware would be more—could we use the patent law to protect the hardware development and the copyright law might be more for the software, data banks, and computer programs? Am I right when I look at the purpose of both laws; that one would apply more than the other?

[Traduction]

Je tire un exemple d'un jugement rendu dans une cause canadienne; si vous achetez un livre de recettes, vous pouvez préparer des repas selon les recettes contenues dans ce livre. Toutefois, d'un point de vue purement pratique, lorsque vous faites affaire avec des machines, comment procéder pour rendre l'information accessible au public tout en protégeant les droits de l'auteur et le mode d'expression?

Permettez-moi de vous donner un autre exemple. Il s'agit d'un cas bien terre-à-terre. Il est maintenant possible de construire des pièces de machinerie ou d'automobile ou d'autres dispositifs très complexes en utilisant des appareils, des outils ou des robots produits par ordinateur. Si un fournisseur de pièces d'automobile canadien veut fabriquer une pièce de remplacement et qu'il en fait faire une analyse conventionnelle pour en obtenir les dimensions, il générera ainsi une base de données et un programme informatique qui, à toutes fins utiles, auront l'air exactement identiques à la base de données et au programme utilisés par le fabricant original de l'automobile. Selon l'état actuel des choses, à moins que les pièces d'automobile ne soient protégées par brevet, il existe une libre concurrence quant aux pièces de remplacement.

Je cite cet exemple pour illustrer un cas où les conséquences d'une protection élargie n'ont pas encore été prévues.

Comme l'a fait remarquer M. Couchman, et je crois qu'il a raison, si vous procédez en vertu de ce que j'appellerais l'approche d'un point de vue criminel, en défendant tout accès non autorisé, etc., il est fort peu probable alors que vous rencontrerez ce genre de problème. J'aimerais faire remarquer que la non-protection, la liberté de l'information, la liberté de concurrence et l'accès libre à la connaissance constituent la règle générale de notre société. Les restrictions de l'accès sont l'exception. Si l'on est trop sévère quant à l'accès aux données informatisées on est menacé de changer cette société pour en adopter une qui soit fermée. Il s'agit là d'éventualités tirées du roman «1984» et je ne veux pas susciter des horreurs, mais néanmoins, il faut être réceptif à cette possibilité car, comme Bruce l'a fait remarquer, la grande différence entre l'information sous forme informatisée dont nous parlons ici et l'information traditionnelle c'est que dans le premier cas il nous est impossible de lire directement les données. Par conséquent, on ne peut «ouvrir le livre», lire les renseignements et se les accaparer.

J'accepterais volontiers de répondre aux questions maintenant, madame le président. M. Couchman est un expert en loi sur le droit d'auteur et je ne prétends aucunement être expert en cette matière. Ma compétence est plus du domaine des brevets et des marques de commerce.

Le président: Croyez-vous que le matériel serait plus—pourrait-on utiliser la Loi sur les brevets afin de protéger le développement du matériel et la Loi sur le droit d'auteur pour protéger le logiciel, les banques de données et les programmes informatiques? Ai-je raison lorsque je songe à l'objectif de ces deux lois? L'une n'est-elle pas plus pertinente que l'autre.

[Text]

Mr. Butler: This gets into probably a fairly useful theoretical discussion. One of the things I think you have to bear in mind is exactly why you are doing it. Several reasons are advanced for property protection. One you are probably familiar with, and that is respect for the moral rights of the creator, or respect for the fact that this is his production and he should have some property right in it. That may be what lies behind the very long periods of protection you get in copyright.

Another argument is the argument that in relation to some works, or some technology, it is enormously easy for the second person to come along and merely take what the first person has done.

• 1135

Economists say that results in a market failure, in the sense that the marketplace does not produce as much of that good as the society needs. People are deterred from creating because of the disadvantage they face when somebody in effect steals what they have created.

In answering your question, the Patent Act grants protection only to those innovations which have merit, and that is to say, they are inventive; they have features which are not obvious to somebody skilled in the art and the term of protection is limited—it is 17 years from grant. That is far shorter than the term of protection granted under copyright.

The Chairman: But for high technology it is a rather long life, 17 years, because . . .

Mr. Butler: Yes.

The Chairman: —most of the things, after 5 years, are almost obsolete.

Mr. Butler: I would agree with you, Madam Chairman. All the terms of protection are ridiculously long. They are excessive.

Now, to go a little further with the patent law, it has been for many years a principle of patent law that while you can get patent covering the practical application of an idea, you cannot get a patent for an abstract theorem or idea. A good example, one that is usually trotted out, is that Einstein could not have obtained a patent on the theory of relativity, but Fermi could have obtained a patent for the bomb, because that was a practical application of it.

Mr. Robinson (Etobicoke—Lakeshore): How about a copyright?

Mr. Butler: Well, he would have got a . . . Einstein would have obtained a copyright in his writings, but he would not have had the exclusive right to his famous formula unless it was in the way in which he wrote it, in his handwriting.

Now, when you apply that principle of patent law to a practical situation where somebody comes in with a computer algorithm or program—they have been rejected here and abroad on the grounds that they are merely abstract theorems.

[Translation]

M. Butler: Nous entrons dans une discussion théorique qui est probablement très utile. L'une des considérations dont il faut tenir compte, c'est le but exact de la protection. Il existe un bon nombre de raisons pour protéger la propriété. Une que vous connaissez probablement très bien, c'est le respect des droits spirituels du créateur, c'est-à-dire le respect du fait qu'il s'agit de sa création et qu'il devrait posséder un certain droit de propriété quant à elle. C'est peut-être l'idée sous-jacente des très longues périodes de protection que l'on obtient en vertu des droits d'auteur.

Un autre argument c'est que dans le cas de certains travaux ou de certaines technologies, il est terriblement facile pour une deuxième personne de simplement s'approprier la création d'une première personne.

Les économistes affirment que cela provoque l'échec du marché, en ce sens que le marché ne produit pas suffisamment de cette marchandise pour répondre aux besoins de la société. Les gens hésitent à créer des choses puisqu'ils sont lésés lorsque d'autres volent de fait le fruit de leur travail.

Pour répondre à votre question, la Loi sur les brevets ne protège que les créations valables, c'est-à-dire celles qui constituent une invention. Ces objets doivent comporter des caractéristiques qui ne sautent pas aux yeux du professionnel du domaine et la période de protection est limitée à 17 ans. Cette période est bien plus courte que celle qui est consentie en vertu des droits d'auteur.

Le président: Mais pour des techniques de pointe, cela est plutôt long, 17 ans, puisque . . .

M. Butler: Oui.

Le président: . . . car la plupart de ces découvertes sont pratiquement périmées après 5 ans.

M. Butler: Je suis de votre avis, madame le président. Toutes les périodes de protection sont ridiculement longues, elles sont excessives.

Mais pour poursuivre au sujet de la Loi sur les brevets, celle-ci se fonde depuis de nombreuses années sur le principe suivant: n'est protégée que l'application pratique d'une théorie, non un théorème abstrait ni une théorie proprement dite. On donne souvent un bon exemple de cette situation lorsqu'on souligne qu'Einstein n'aurait pu obtenir de brevet sur la théorie de la relativité, mais que Fermi aurait pu l'obtenir pour sa bombe qui constituait une application très pratique du principe mentionné.

M. Robinson (Etobicoke—Lakeshore): Qu'en est-il des droits d'auteur?

M. Butler: Eh bien, il aurait obtenu—Einstein aurait obtenu des droits d'auteur sur ses écrits, mais il n'aurait pas bénéficié du droit exclusif sur sa formule célèbre sauf sur sa rédaction, établie de sa propre main.

Mais, si vous appliquez ce principe de la Loi sur les brevets à une situation pratique comme celle où quelqu'un présente un algorithme ou un programme informatique—on a rejeté ces demandes ici et à l'étranger pour le motif qu'il ne s'agit-là que

[Texte]

But if somebody comes in with an algorithm which is used to effect a particular industrial result—for instance, there is a patent on a method for curing rubber tires, in which there is an algorithm which explains how you compute the various relative temperatures to tell the machinery to open the mould and eject the tire, once it is cured—then those claims have been allowed.

Now, I would suggest that if you are going to grant some form of protection for algorithms, if you are seriously going to do this, the patent issue should be rethought. Maybe you should be considering giving some form of protection for computer algorithms, because the reasons for rejecting those claims tend to be legalistic.

To give you another example—and this is going down the road; we are straying somewhat from criminal law—you frequently find when you go through one of these exercises to the very end that there was an easier way of doing it all along. Now, I think the problem arises in this way. If I sell or rent to you a computer program or data base, and I get you to promise me that you will not let anybody else have access to it, and if you turn around and let somebody have access to it, or they somehow get access to it, I cannot sue that person in the civil courts. Why? Because there is no contractual link between myself and that third person. I have some hope, under the developing civil law, if I can show that the person who stole it knew that he was infringing or violating my rights.

Now the reason I am posing this question is, if I asked the question under a different scheme, would you be prepared to prosecute or permit people to sue individuals who are totally innocent, who innocently come into possession of something which is an infringement? I think the answer to that is no.

• 1140

So another approach you can take, I am suggesting to you, is to change the trade secrecy laws so that persons who knowingly interfere with the trade secrets of other parties can be solely liable. It is far easier than a more elaborate system.

The other thing I would leave you with is... and Madam Chairman, you certainly pointed it out—if you accept the market failure argument, that people will not produce these things unless they have protection, the necessary period of protection is relatively short. I would not want to put figures on it, but I think under current interest rates it is probably about three years. If you cannot recover your investment in that relatively short period of time, you never will.

The other observation I would leave you with is that for Canadian high technology, the major market is the United States. Very few people in their right minds would be investing

[Traduction]

de théorèmes abstraits. Mais si l'on présente un algorithme qui est utilisé pratiquement pour obtenir un résultat industriel—par exemple, il y a un brevet sur la vulcanisation des pneus de caoutchouc parce que celle-ci se fait au moyen d'un algorithme qui régit le calcul des diverses températures relatives et commande à l'équipement d'ouvrir le moule et d'éjecter le pneu une fois la vulcanisation terminée—alors, ces demandes de brevet ont été agréées.

Il faudrait maintenant préciser que si l'on veut consentir une forme de protection aux algorithmes, il faudrait alors réexaminer sérieusement toute la question de l'octroi de brevets. Peut-être pourrait-on envisager d'accorder un genre de protection aux algorithmes informatiques, vu que les motifs pour lesquels on a rejeté ces demandes jusqu'à maintenant sont plutôt de nature légaliste.

Pour vous donner un autre exemple, mais nous nous éloignons quelque peu ici du droit criminel, on s'aperçoit fréquemment lorsqu'on approfondit ces questions qu'il y aurait eu une façon plus facile de procéder. Mais voici comment le problème se présente, selon moi. Si je vous vends ou vous loue un programme informatique ou une base de données et que j'obtiens de vous la promesse que vous ne permettrez à personne d'autre d'y avoir accès, alors que par la suite, vous laissez n'importe qui s'en servir ou d'autres y ont accès d'une façon ou d'une autre, je ne peux vous poursuivre devant les tribunaux civils. Pourquoi? Parce qu'il n'y a aucun lien contractuel entre moi et cette tierce personne. Le seul espoir qui me reste, en raison de l'évolution du droit civil, c'est de pouvoir démontrer que l'auteur du vol savait qu'il transgressait ou violait mes droits.

Mais la raison pour laquelle je pose cette question est la suivante: si je posais cette question dans un contexte différent, seriez-vous prêts à poursuivre des gens complètement innocents ou à permettre d'autres de le faire, c'est-à-dire des gens qui entrent innocemment en possession de quelque chose qui constitue une infraction? Je crois que la réponse est non.

Mais une autre façon d'aborder la question serait, selon moi, de modifier les mesures législatives sur le secret commercial de façon à ce que seules soient passibles de poursuite les personnes qui entravent sciemment les secrets commerciaux d'autres personnes. Cela serait beaucoup plus facile qu'un système plus complexe.

Une autre observation que je souhaiterais faire, et que vous l'avez certainement déjà soulignée, madame le président, si l'on accepte l'argument de l'échec du marché, c'est-à-dire que les gens ne produisent pas ces choses à moins de bénéficier d'une protection, la période de protection nécessaire demeure relativement courte. Je ne voudrais pas préciser de chiffres, mais je crois qu'en vertu des taux d'intérêt en vigueur, il s'agit probablement d'environ trois ans. Si l'on ne peut recouvrer son placement dans ce délai relativement court, on ne le fera jamais.

Autre remarque: le principal marché des techniques de pointe canadiennes se trouve aux États-Unis. Très peu de gens sensé investiraient d'importantes sommes d'argent dans de

[Text]

large sums of money in new products which they could not sell in the United States and abroad; our market is not large enough. So it is a bit of a delusion to think major changes in Canadian law are going to have a substantial impact on the behaviour of Canadian business. It is the rights they obtain abroad that are important. You may be interested to know in my field more Canadians obtain patents in the United States than they do at home. The usual practice for Canadian inventors is to apply for a patent in the United States first. Then if it looks as if they have something good, they will consider applying here. And that is totally rational, totally sensible, behaviour.

Maybe I am muddying the water a little. I guess I am building up to an observation; and that is—I am speaking totally and personally now; this is not a department view. We are between a rock and a hard place, because our ministers of course want to do something in relation to copyright, and we do not want to prejudice people's positions in one way or the other. But I think when you move in this sort of area and you create property rights, you always have to ask yourself, what happens if we are wrong? What happens if we make a mistake? How do we get out of it?

It seems to me if you have legislation which creates penal sanctions for people who improperly access other people's data bases, etc., and it turns out that it is not a good idea for some reason, it is relatively easy to amend or appeal that law. If you create a property right and that property right has a long term, then the normal rules of respect for property rights in terms of the transitional provisions make it extremely difficult to repeal that legislation. To give you an example, if the term of protection for a computer program were 50 years, or the life of the author plus 50 years, then I do not think any politicians will be the slightest bit interested in a repeal measure, because they would all be long dead before the thing ever took effect. It is fairly obvious.

I guess I am advocating what I would call a conservative approach towards the thing, and that is, proceed carefully and try to avoid making mistakes.

Mr. Robinson (Etobicoke—Lakeshore): That is a small "c", I hope.

Mr. Butler: That is right.

It is from my former life, when I used to represent doctors. In medical practice, when you are prescribing a medicine, for instance, if you have a patient with a stroke and you can treat them by giving them an anticoagulant, you always have to bear in mind if it does not work you might have to operate, and the patient would then bleed to death. So the kind of approach I would like is a careful one.

I have talked overly long here. I think you probably are basically interested in questioning Bruce.

[Translation]

nouveaux produits qu'ils ne pourraient vendre aux États-Unis et à l'étranger; car notre marché n'est pas assez important. C'est donc quelque chose illusoire de croire qu'en modifiant sensiblement la loi canadienne, on provoquerait un changement substantiel du comportement des gens d'affaires du Canada. Ce sont les droits qu'ils obtiennent à l'étranger qui importent. Vous serez peut-être intéressés d'apprendre que dans mon domaine, les Canadiens obtiennent plus de brevets aux États-Unis que dans leur propre pays. C'est l'usage pour les inventeurs canadiens de présenter une demande de brevet d'abord aux États-Unis. Puis, s'il semble que leur invention est bonne, ils envisageront alors d'en présenter une ici. Et cette façon de procéder est absolument rationnelle, absolument sensée.

Mais, peut-être que je brouille quelque peu les cartes. Cependant, je crois que tout cela nous mène à une observation—je ne parle ici que pour moi-même et nom au nom du Ministère. Nous sommes ici entre l'enclume et le marteau puisque nos ministres veulent évidemment faire quelque chose au sujet des droits d'auteur tandis que nous ne voulons léser personne d'aucune façon. Selon moi, lorsqu'on touche un secteur comme celui-là pour créer des droits de propriété, il faut toujours s'interroger sur ce qui se produira, en cas d'erreur? Qu'advient-il, si nous nous trompons? Comment en sortir?

Il me semble que si l'on adopte une mesure législative pour pénaliser ceux qui accèdent fautivement aux bases de données d'autres gens, etc., et que cette mesure se révèle inopportune pour une raison ou pour une autre, il est relativement facile de modifier ou de retirer cette loi. Mais, si vous créez un droit de propriété qui s'étend sur une longue période, les règles habituelles d'application des dispositions provisoires concernant le respect des droits privés sont elles qu'il est extrêmement difficile de retirer la mesure législative inopportune. Pour vous donner un exemple, si le délai de protection d'un programme informatique est de 50 ans ou équivalait à la durée de la vie de l'auteur plus de 50 ans, je crois qu'aucun législateur ne sera alors le moins intéressé à retirer cette mesure puisqu'il serait déjà mort avant que sa décision puisse entrer en vigueur. Cela est assez évident.

Je pense bien préconiser ce que j'appellerais une approche prudente, c'est-à-dire qu'il faut procéder soigneusement et tenter d'éviter toute erreur.

M. Robinson (Etobicoke—Lakeshore): Une attitude qui n'est pas fondée sur la partisanerie politique, j'espère.

M. Butler: En effet.

Jadis, je représentais des médecins, lorsqu'un médecin prescrit un médicament, supposons, par exemple qu'il donne un anticoagulant à quelqu'un qui vient de subir une crise cardiaque, il doit toujours se rappeler que s'il devait procéder à une intervention chirurgicale ce malade pourrait mourir au bout de son sang. Alors l'attitude que je préconise est donc une attitude prudente.

J'ai beaucoup trop parlé. Je pense que vous aimeriez peut-être maintenant interroger Bruce.

[Texte]

The Chairman: Just another question; and I will refer to Ken, just to clarify—we have been clarifying words since we started this committee.

• 1145

Would you treat it with the copyright law—I mean the information stored in computer, the data bank—differently from the programs? I mean those who are developing the instructions to work on these data banks. Could you say that copyright coverage might be used for the programs, but as for information... well, the information is there and, after hearing of freedom of information, there is no need and, certainly, no practicality in trying to protect that information.

Mr. Butler: I will let Bruce Couchman answer this, but I will make just two observations.

Although I am not a computer programmer, I am of the view that, as a thing as opposed to the purpose for which it is put, it is a physical object. There is no difference between a program and a data base. I realize that dichotomy is always being put to you. It is assumed; but it is a difference which arises from the purpose for which the thing is intended or the purpose to which it is put. But indeed, physically examined and seen from the point of view of a judge who now has to decide whether this thing is a data base or a program, I do not think there is any material difference between the two.

That is a personal opinion. Now other people might think...

The Chairman: I think that is right. There is no problem. They use the same hardware...

Mr. Butler: That is right.

The Chairman: —and the same micro-chip.

Mr. Butler: Sure. I mean, the information in the micro-chip is that if you do things in the following sequence, you get this result. Is that an algorithm or is it a data base? So by answering that question I guess I cannot go any further. I do not know what it is!

Mr. Couchman: I think in terms of the current copyright law, the nature of the protection would be the same—that is, both of them face the problem that they are in a form which human beings cannot see or understand. So I have a feeling that if the courts found that one were not protected, they would find that the other was not protected also, and vice versa.

Obviously there are other problems which computer programs have in terms of the current law. For example, they may amount to a mathematical formula. They may be simply an expression of a very basic concept. So conceivably a computer program, if it is of a very, very fundamental nature, even in its written-out form may have more difficulty attracting copyright protection. It is the same problem that Tony Butler mentioned with Einstein's formula. The basic mathematical formula is not going to get protection; but anything more elaborate than that would get protection in its written-

[Traduction]

Le président: Juste une autre question, puis je passerai à Ken. Une seule clarification: depuis le début des travaux du comité, nous avons précisé beaucoup de mots.

Dans la Loi sur les droits d'auteur, est-ce que vous les traiteriez—c'est-à-dire les renseignements stockés dans l'ordinateur, la base de données—différemment des programmes? Je pense ici aux auteurs d'instructions concernant les banques de données. Pourrait-on dire que les droits d'auteur pourraient s'appliquer aux programmes tandis que pour ce qui est des renseignements... eh bien, les renseignements sont là et, lorsqu'on est au courant d'abord à l'information, il n'est pas nécessaire et, certainement, pas pratique de tenter de protéger les renseignements.

M. Butler: Je laisserai Bruce Couchman répondre à cette question, mais je ferai seulement deux observations.

Bien que je ne sois pas un programmeur informatique, je crois qu'en tant qu'entité par opposition à ce à quoi elle sert, elle constitue un objet matériel. Il n'y a pas de différence entre un programme et une base de données. Je me rends compte qu'on m'oppose toujours cette dichotomie. Il s'agit-là d'une présomption? C'est une différence qui découle du but de la chose ou de son utilisation. Mais, du point de vue matériel et juridique lorsqu'il faut décider si telle chose est une base de données ou un programme, je ne crois pas qu'il y ait de différence réelle entre les deux.

C'est une opinion personnelle. D'autres personnes pourraient croire que...

Le président: C'est vrai, il n'y a pas de difficulté. Ils utilisent le même matériel...

M. Butler: Cela est vrai.

Le président: —et la même microplaquette.

M. Butler: Bien sûr. Les renseignements qui se trouvent dans la microplaquette sont tels que si l'on procède dans l'ordre voulu, on obtient le résultat. S'agit-il d'un algorithme ou d'une base de données? Donc, avec cette question je ne puis en dire davantage. Je ne sais pas la réponse:

M. Couchman: En ce qui concerne la loi actuelle sur les droits d'auteur, je crois que la nature de la protection est la même. C'est-à-dire que tous les deux comportent une difficulté en ce sens qu'ils se présentent sous une forme que l'être humain ne peut voir ni comprendre. Je pense donc que si les tribunaux décidaient que l'un n'est pas protégé, ils en feraient autant pour l'autre, et réciproquement.

Manifestement, la loi actuelle présente d'autres difficultés, en ce qui concerne les programmes informatiques. Par exemple, ces programmes peuvent correspondre à une formule mathématique. Ils ne sont parfois que la simple expression d'une théorie très fondamentale. Il se peut donc qu'un programme informatique qui n'est pas très, très fondamental ne puisse, même sous sa forme écrite, bénéficier de la protection accordée en vertu des droits d'auteur. C'est le même genre de difficulté que celle qu'a mentionné Tony Butler au sujet de la formule d'Einstein. On ne peut protéger la formule mathématique.

[Text]

out form. So under the current law, the status would be basically the same.

In terms of possible law reform, looking down over the years there may be reasons why they should be treated differently. Certainly they have completely different industrial and commercial significance. For example, the World Intellectual Property Organization, which is an agency of the United Nations, is currently looking at a possible international treaty for the protection of computer programs. And they recognize that the reasons why you want to protect programs, the duration of protection, the types of infringing acts, may be completely different for computer programs from those for data bases. For example, they would consider making the use of a program an infringing act; whereas the use of information as such, the use of a data base, the use of something protected by copyright, is not an infringing act under any current copyright laws. So in theory there are reasons why one would want to treat them very differently.

Another difference is that computer programs can be developed in a sense in the privacy of a room. That is, you can come up with a computer program which is identical to someone else's computer program just on your own. And therefore the problems of proving independent creation, and proving to a court that in fact you thought it up on your own, are very difficult with computer programs. They are much more difficult than with data bases, because with data bases you can at least introduce evidence into the court that you went out and collected the information; that you interviewed people or whatever, and got the information through your own efforts. With computer programs potentially there are much greater problems in proving independent creation.

The Chairman: So you see some future of our coming up with an international treaty? Then we could be on the same ground; then we could legislate from that; we could even invent new legislation?

• 1150

Mr. Couchman: It is possible, for example, that if a treaty came into existence Canada would want to model its law in some way after the treaty so we could get the advantages of protection in other countries.

Obviously, we have a certain limited protection now even under copyright law, in the sense that copyright law, because it is interpreted differently in different countries, grants a certain protection. For example, speaking very generally, Canadian programs receive more protection in the United States now, or at least receive more explicit protection in the United States, than they do in Canada. It may be that there will be court cases in Canada which will result in programs receiving very extensive protection, but at least at present they do receive

[Translation]

matique de base mais seulement quelque chose de plus développé, sous sa forme écrite. En vertu de la loi en vigueur, la situation serait donc fondamentalement la même.

Pour ce qui est d'une refonte possible de la loi, si on examine ce qui s'est fait au cours des années, il pourrait y avoir des raisons de les traiter différemment. Leur rôle industriel et commercial est certainement tout à fait différent. Par exemple, l'Organisation mondiale pour la propriété intellectuelle, organisme des Nations unies, étudie actuellement la possibilité d'un traité international de protection des programmes informatiques. Cet organisme admet que les raisons pour lesquelles on veut protéger les programmes, la durée de la protection, les genres d'infractions, peuvent différer complètement dans le cas des programmes informatiques et dans celui des bases de données. Par exemple, on envisagerait de faire de l'utilisation d'un programme ou infraction tandis que l'utilisation des renseignements comme tels, l'utilisation d'une base de données, l'utilisation de quelque chose qui est protégé par des droits d'auteur, n'est pas reconnue comme une infraction par les lois actuelles concernant les droits d'auteur. Donc, théoriquement, il y a des raisons pour traiter ces deux éléments très différemment.

Une autre différence provient de ce que les programmes informatiques peuvent être mis au point, pour ainsi dire, dans le secret de sa chambre. C'est-à-dire que l'on peut mettre au point un programme informatique qui est identique à celui d'un autre. Par conséquent, il est très difficile, dans le cas de programmes informatiques, de démontrer qu'il s'agit d'une innovation réelle et de faire la preuve devant un tribunal qu'il s'agit bien de sa propre invention. Cela est encore beaucoup plus difficile pour les bases de données. Dans ce cas, on pourrait quand même présenter au tribunal la preuve qu'on s'est déplacé pour recueillir les renseignements, qu'on a rencontré des gens et le reste, et que l'on a obtenu les renseignements à la suite d'un travail personnel. Il est beaucoup plus difficile de démontrer qu'un programme informatique constitue une création propre.

Le président: Vous croyez donc qu'il est possible qu'on en arrive dans l'avenir à un traité international? Nous pourrions alors être sur le même pied, nous pourrions adopter une mesure législative à partir de ce traité, nous pourrions même adopter une nouvelle loi?

M. Couchman: Par exemple, il est possible que si un traité était conclu, le Canada voudrait s'en inspirer pour légiférer de façon que nous puissions jouir de la protection offerte à l'étranger.

Evidemment, même les lois actuelles sur le droit d'auteur accordent une protection limitée; en effet, comme leur interprétation diffère selon les pays, elles assurent une certaine protection. Par exemple, dans l'ensemble, les programmes canadiens sont actuellement davantage protégés aux États-Unis ou du moins, font l'objet de mesures de protection plus explicites aux États-Unis qu'au Canada. Il se peut que des causes portées devant les tribunaux canadiens se traduisent éventuellement par une protection complète des programmes;

[Texte]

protection in the United States which is at least more explicit than in Canada. Canadian programs also probably receive more protection in Japan than they do in Canada, simply because the Japanese courts have ruled that their copyright act, even though it makes no mention of computer programs, in effect extends to them.

So even if we did not join such a treaty we would receive certain benefits of other countries' copyright law or patent law that happened to apply.

I would definitely feel that if a treaty did come into existence, we would want very carefully to examine our law to see if we would have to change certain things to take advantage of that treaty.

The Chairman: Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman.

So what you are really saying then, Mr. Couchman, is that you cannot really protect something that you cannot prove when you are talking about information stored in a computer.

Mr. Couchman: That you cannot prove . . . ?

Mr. Robinson (Etobicoke—Lakeshore): You cannot prove that it is original.

Mr. Couchman: You can protect it in principle. What I am saying is that it will be much more difficult to prove independent creation with certain types of computer programs.

My understanding, for example, is that with basic accounting systems that are developed for, say, law offices and medical offices it is very difficult for a developer of that program to prove that someone else who has developed a very similar program has not copied it, because two people sitting down to solve a certain problem, how should that accounting system be set up, may develop very, very similar computer programs; and in some cases, of course, the second firm may have former employees of the first firm.

Now, in principle the nature of the copyright protection, to the extent it exists, is exactly the same. But the problems of proving independent creation before a court are very difficult. My understanding is that, for example, some companies would have a very difficult time getting, say, bank loans on the basis that they had a particular very simple accounting system. To the extent that that might be protected by copyright, how do you prove that someone else who has a very similar system has developed it independently or copied from you? It is extremely difficult.

Mr. Butler: I think I understand the structure of what is going on. You may be talking at cross purposes. Bruce is concerned with somebody who buys or leases a program or a person who has developed a program and is sued by somebody else accused of being an infringer. I think that is what he is concerned with. Am I right? Yes. It got twisted around, I think, as we were talking back and forth.

[Traduction]

pour l'instant, toutefois, ils reçoivent aux États-Unis une protection qui est effectivement plus explicite qu'au Canada. Il est probable que les programmes canadiens soient également davantage protégés au Japon qu'au Canada, tout simplement parce que les tribunaux japonais ont décidé que leur loi sur le droit d'auteur s'appliquait en fait aux programmes informatiques même s'il n'en est fait aucune mention.

Ainsi, même si nous ne ratifions pas un pareil traité, nous profiterions d'une certaine façon des lois sur le droit d'auteur et sur les brevets en vigueur dans d'autres pays.

Je suis absolument d'avis que s'il y avait un traité, nous voudrions examiner très attentivement notre législation pour déterminer si nous aurions avantage à en modifier certains éléments pour tirer profit de ce traité.

Le président: Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président.

Alors, lorsque vous parlez de renseignements stockés dans un ordinateur, vous dites en réalité, monsieur Couchman, qu'il n'est pas vraiment possible de protéger quelque chose qu'on ne peut pas démontrer.

M. Couchman: Qu'on ne peut pas démontrer . . . ?

M. Robinson (Etobicoke—Lakeshore): On ne peut pas démontrer qu'il s'agit d'une innovation.

M. Couchman: La protection est possible en théorie. Je dis simplement qu'il sera beaucoup plus difficile de prouver une véritable création pour certains types de programmes informatiques.

Prenons, par exemple, le cas du réalisateur d'un système de comptabilité de base pour un cabinet d'avocats ou de médecins. À mon avis, ce dernier aura beaucoup de mal à prouver que le programme très similaire mis au point par quelqu'un d'autre est un plagiat. En effet, deux personnes sont en présence d'un problème donné et doivent élaborer un système de comptabilité pour le régler; elles peuvent très bien écrire des programmes informatiques extrêmement similaires. Dans certains cas même, une des entreprises peut avoir à son service des personnes autrefois à l'emploi de l'autre entreprise.

Maintenant, en principe, la nature de la protection conférée par le droit d'auteur, dans la mesure où elle existe, est exactement la même. Toutefois, il est très difficile de prouver une véritable innovation devant les tribunaux. Toujours selon moi, certaines sociétés auraient beaucoup de mal à obtenir, par exemple, des prêts bancaires en raison du fait qu'elles ont un système de comptabilité très simple. Dans la mesure où celui-ci est protégé par droit d'auteur, comment démontrer qu'une autre personne qui a un système très similaire a copié sur vous? Cela est très difficile.

M. Butler: Je crois comprendre ce qui se passe. Vous avez peut-être des objectifs opposés. Bruce est préoccupé par le cas d'une personne qui achèterait ou louerait un programme ou qui aurait élaboré un programme et serait poursuivie par quelqu'un qui l'accuse d'intrusion. Je crois que c'est ce qui le préoccupe. Aie-je raison? Oui. Je crois que vos propos ont été dénaturés dans le cours de la discussion.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): Do I understand that at present there is no international treaty on intellectual property?

Mr. Couchman: There are copyright treaties. Canada belongs to two copyright treaties. There is a patent treaty. But there is no treaty dealing specifically with computer software.

Mr. Robinson (Etobicoke—Lakeshore): If there was a treaty, would it include copyright, patent, industrial design, trade marks as well—all of these?

Mr. Couchman: The current proposal, which is still at a very early stage of development, would be in addition to whatever other forms of protection existed—that is, in computer programs; that is, if a particular country granted copyright protection to computer programs it would still have to grant copyright protection, but in addition it would grant this other form of protection.

Although this is still at a very early stage in various courts, I would imagine that in some countries interpreting their current copyright laws it will be held that those laws as they exist do protect computer programs or data bases in machine-readable form even though they are not mentioned in the copyright legislation of those countries, while it may be that in other countries the courts will hold that such data bases and programs are not protected under the existing copyright laws.

Now, to the extent that these things are protected under copyright laws of our treaty partners, Canadian works would also be protected in those other countries. The proposal for treaty would be for something completely new and different, which would be in addition to copyright or patent protection, and it would have a different nature from copyright or patent protection.

• 1155

Mr. Robinson (Etobicoke—Lakeshore): Is it anticipated that there would be greater protection under the international treaty than there is under our present laws?

Mr. Couchman: The proposal would grant greater protection than exists under current Canadian laws, but it would be for a shorter term.

Mr. Robinson (Etobicoke—Lakeshore): But this would only apply to software as far as the computer . . .

Mr. Couchman: That is correct; it would not apply to data bases.

Mr. Robinson (Etobicoke—Lakeshore): Yes. All right.

I think it was Mr. Butler who was talking about the moral rights of the creator. I suppose you are really suggesting moral suasion was going to be the answer. But really we are not talking about moral rights, are we? We are talking about legal rights.

[Translation]

M. Robinson (Etobicoke—Lakeshore): Dois-je comprendre qu'à l'heure actuelle, il n'y a pas de traité international sur la propriété intellectuelle?

M. Couchman: Il existe des traités sur le droit d'auteur. Le Canada a ratifié deux de ces traités. Il y a aussi un traité sur les brevets. Toutefois aucun traité ne porte précisément sur le logiciel.

M. Robinson (Etobicoke—Lakeshore): Un pareil traité, s'il existait, engloberait-il le droit d'auteur, les brevets, le dessin industriel ainsi que les marques de commerce?

M. Couchman: Le projet actuel à peine ébauché viendrait s'ajouter à toutes les autres mesures de protection déjà prévues en matière de programmes informatiques; autrement dit, si un pays donné accordait une protection par droit d'auteur aux programmes informatiques, il devrait non seulement assurer cette protection, mais également appliquer les autres mesures déjà établies.

Bien que les différents tribunaux commencent à peine à être saisis de ces cas, j'imagine que, dans certains pays, où on leur a demandé d'interpréter les lois sur le droit d'auteur en vigueur, ils vont conclure que ces lois, telles qu'elles sont libellées, protègent effectivement les programmes informatiques ou les bases de données sous forme exploitable par machine même s'il en est pas fait mention dans la législation. Par contre, les tribunaux d'autres pays vont soutenir que ces bases de données et ces programmes ne sont pas protégés aux termes des lois sur le droit d'auteur actuelles.

Or, dans la mesure où ces oeuvres sont protégées en vertu des lois sur le droit d'auteur en vigueur dans les autres pays qui ratifieraient le traité, les ouvrages canadiens seraient également protégés dans ces pays. Le traité régirait quelque chose de tout à fait nouveau et différent qui viendrait s'ajouter à la protection par le droit d'auteur ou le brevet; la nature de la protection accordée en vertu du traité serait différente de celle qui est conférée par le droit d'auteur ou le brevet.

M. Robinson (Etobicoke—Lakeshore): La protection en vertu du traité international serait-elle supérieure à celle qui est prévue aux termes de nos lois actuelles?

M. Couchman: Le projet de traité assure une protection supérieure à celle qui est actuellement offerte aux termes des lois canadiennes, mais pour une période plus courte.

M. Robinson (Etobicoke—Lakeshore): Mais ce traité ne s'appliquerait qu'au logiciel . . .

M. Couchman: C'est exact; il ne viserait pas les bases de données.

M. Robinson (Etobicoke—Lakeshore): Oui. Très bien.

Je pense que c'est M. Butler qui a parlé du droit moral du créateur. Je suppose que ce que vous vouliez vraiment dire était que la pression morale allait être la réponse. Mais en fait, il n'est pas question de droit moral ici, n'est-ce pas? Il est question de droits civils.

[Texte]

Mr. Butler: I agree; but what I am talking about is the rationale for your doing it. In the case of an author of a book, we give a very long period of protection, I think for very human reasons. It is a kind of pension for an author. They are human-oriented reasons. When you talk about giving protection to IBM, I do not think the human reasons are there. It is not corporate anthropomorphism—that you treat corporations as if they are human beings, for all purposes. I was just talking about when you have truly artistic works, there is a tendency to relate the term of protection to the lifespan of the creator and his family. That is where you get this long period.

I wanted to mention something to you in the international sphere, because you are interested. There are two basic copyright conventions: the Berne Convention, to which Canada is a party, and the Universal Copyright Convention, to which we are also a party. Berne can be characterized as a non-formalities convention. We cannot under Berne impose formalities such as registration, etc., but under the Universal Copyright Convention we can.

The United States is a member of UCC only; it is not a member of Berne... the effect of which is that in the United States, although they recognize copyright in computer programs and data bases, they impose formalities. If we were to extend copyright protection in Canada, explicitly, then we would be caught by the provision under Berne that we could not impose formalities.

So it is a situation where we cannot conform with the American law exactly, because they are governed by a different treaty. That has a practical implication when you are concerned about the rights and interests of users, because in the United States there is a register they can consult; in Canada there would not be.

Mr. Robinson (Etobicoke—Lakeshore): Do you feel that this international treaty might resolve the difficulty?

Mr. Butler: This is getting to be highly technical, but there is a problem in the industrial property treaties where countries move from one text of a treaty to another, or from one treaty to another, which I think you can illustrate by the juxtaposition of the Berne and UCC conventions.

The question, and it is a question I am going to leave open, because I do not know the answer to it, and we probably will not know for many years, is that if a country like Canada, which is governed by Berne, ratifies a new treaty, say the WIPO Treaty on computer software, and that new treaty imposes obligations not found in Berne, but relieves us of some obligations found in Berne, do we then in effect escape from Berne in terms of those obligations, or are we bound by both?

[Traduction]

M. Butler: Je suis d'accord avec vous, mais je veux parler de ce qui vous pousse à le faire. Nous accordons à l'auteur d'un livre une très longue période de protection, à mon avis pour des raisons très humanitaires. Il s'agit en quelque d'une pension pour l'auteur. Nous sommes animés par des sentiments humanitaires. Lorsque vous parlez d'accorder une protection à IBM, je ne pense pas que cela soit pour les mêmes motifs. Il ne s'agit pas d'anthropomorphisme d'entreprise... à toutes fins pratiques que vous traitiez les entreprises comme des êtres humains. Je faisais simplement allusion au fait que dans le cas d'oeuvres vraiment artistiques, on a tendance à établir la période de protection en fonction de l'espérance de vie du créateur et de sa famille, d'où la longue période.

Comme vous vous intéressez à la chose, j'aimerais vous parler de deux conventions internationales de base en matière de droits d'auteur: la Convention de Berne et la Convention universelle sur le droit d'auteur, la Convention de Berne ne nous permet pas d'imposer des modalités telles que l'enregistrement, et cetera.

Les États-Unis ont ratifié uniquement la Convention universelle sur les droits d'auteur parce que, bien qu'ils reconnaissent le droit d'auteur pour les programmes informatiques et les bases de données, ils imposent des modalités. Si nous devions étendre la protection conférée par le droit d'auteur au Canada, nous contreviendrions à la disposition de la Convention de Berne en vertu de laquelle il est interdit d'imposer des modalités.

Il s'agit donc d'une situation où nous ne pouvons pas observer rigoureusement la législation américaine, parce que les mêmes traités ne s'appliquent pas aux deux pays. Cela a une incidence réelle lorsque vous êtes préoccupé par les droits et les intérêts des utilisateurs parce qu'aux États-Unis les utilisateurs peuvent consulter un registre, alors qu'au Canada c'est impossible.

M. Robinson (Etobicoke—Lakeshore): Pensez-vous que ce traité international peut régler le problème?

M. Butler: Il s'agit là d'une question très complexe. En effet, les différents traités sur la propriété industrielle posent le problème suivant: les pays passent d'un texte de traité à un autre ou d'un traité à un autre. Je crois que le cas de la Convention de Berne et de la Convention universelle sur le droit d'auteur en est un bon exemple.

La question est, il s'agit d'une question à laquelle je ne vais pas répondre puisque je ne connais pas la réponse et que nous ne la connaissons probablement pas avant bien des années, concerne le cas où un pays comme le Canada, qui est régi par la Convention de Berne, ratifie un nouveau traité, par exemple le traité de l'OMPI sur le logiciel, et que ce nouveau document établit des modalités qui ne figurent pas dans la Convention de Berne, mais nous libèrent de certaines obligations énoncées dans celle-ci. Pouvons-nous alors effectivement nous soustraire des obligations contractées par la ratification de la Convention de Berne ou sommes-nous liés par les deux accords?

[Text]

There are a number of countries in this position. The U.K. in relation to performing rights got itself into this jam, because they are bound by the Rome Convention, which requires them to protect the interests of performers in records.

• 1200

They are also members of Berne. The question arises, then, when the U.K. gives performers—that is, people who play in the band and sing on the tape—copyright in their performances, are they obliged to give Canadians the same rights under Berne? Canada is not a member of the Rome Convention.

Mr. Robinson (Etobicoke—Lakeshore): It sounds like a conflict-of-law situation, in which I do not think we want to get involved.

Mr. Butler: That is exactly it, and that is why I cannot give you a straight answer on it.

Mr. Robinson (Etobicoke—Lakeshore): Mr. Butler, you are a specialist in patent law, and Mr. Couchman, you are a specialist in copyright. Can you tell us what kinds of amendments you see to both of those acts which might be helpful in resolving the dilemma we are in today? I take into account that although you have mentioned the Industrial Design Act and the Trade Marks Act, you feel neither of these can be helpful, although you did refer to the trade secrecy law, and maybe you would like to expand on that a bit as well.

Mr. Couchman: I am not sure it would be appropriate for us to reveal, in open forum, proposals with respect to computer software in the Copyright Act. There definitely are provisions which will be in the Copyright Act, explicitly dealing with programs and data bases in machine-readable form. But I do not believe it would be appropriate to reveal these, since the...

Mr. Robinson (Etobicoke—Lakeshore): Surely you can tell us generally whether you are talking about new definitions for the same old words like property, data, and information and so on, and how this is going to relate to the software we are talking about.

Mr. Couchman: Right. Basically, I think the feeling is there should be some form of explicit protection in copyright law. As I said, I do not believe I can get into the details in an open forum, but I think the feeling is that there should be some form of explicit protection.

There is also a feeling, probably, that there are certain things about traditional copyright protection which may not be appropriate in all cases. That is, it may be necessary to fashion certain special types of provisions with respect to material in

[Translation]

Un certain nombre de pays se trouvent dans cette position. Le Royaume-Uni s'est mis dans cette impasse avec les droits d'exécution et de représentation parce qu'il est lié par la Convention de Rome qui l'oblige à protéger les artistes interprètes ou exécutants qui font des enregistrements sur disque.

Ils sont également membres de la Convention de Berne. La question se pose, alors, quand le Royaume-Uni donne à des artistes, c'est-à-dire à des gens qui jouent dans un orchestre et chantent et sont enregistrés sur bande magnétique, des droits d'auteurs en vertu de la Convention de Berne. Doit-on donner aux Canadiens les mêmes droits? Le Canada n'a pas signé l'Acte de Rome.

M. Robinson (Etobicoke—Lakeshore): Cela ressemble à une situation de conflit de lois, et je pense que nous ne voulons pas nous engager dans cette voie.

M. Butler: C'est exactement ça, et voilà pourquoi je ne peux pas vous donner de réponse claire à ce sujet.

M. Robinson (Etobicoke—Lakeshore): Monsieur Butler, vous êtes spécialiste en droit des brevets, et vous, monsieur Couchman, vous êtes spécialiste de la législation sur le droit d'auteur. Pouvez-vous nous dire quelles sortes de modifications l'on pourrait apporter dans ces deux domaines pour sortir du dilemme dans lequel nous nous trouvons aujourd'hui? Je note que vous avez mentionné la Loi sur les dessins industriels et la Loi sur les marques de commerce en disant que, selon vous, aucune des deux ne peut être utile, mais vous avez aussi fait allusion à la Loi sur les secrets commerciaux. Peut-être voudriez-vous donner un peu plus de détails à ce sujet également?

M. Couchman: Je ne crois pas qu'il conviendrait que nous révélions dans un débat public, les propositions qui concernent le logiciel informatique dans la Loi sur le droit d'auteur. Il y a assurément des dispositions qui seront contenues dans la Loi sur le droit d'auteur, traitant explicitement des programmes et des bases de données assimilables par une machine. Mais je ne crois pas qu'il serait convenable de les révéler, étant donné que...

M. Robinson (Etobicoke—Lakeshore): Vous pouvez certainement nous dire si, en général, vous parlez de nouvelles définitions des mêmes vieux mots tels propriété, données et information, etc., et quel rapport cela va avoir avec le logiciel dont nous sommes en train de parler.

M. Couchman: D'accord. Fondamentalement, je pense qu'on a le sentiment qu'il devrait y avoir une forme quelconque de protection explicite dans les lois sur le droit d'auteur. Ainsi que je l'ai dit, je ne crois pas qu'il faille entrer dans les détails ici, mais je pense qu'on a le sentiment qu'il devrait y avoir une forme quelconque de protection explicite.

On a également le sentiment, probablement, que certaines dispositions concernant la protection traditionnelle par les droits d'auteur ne sont peut-être pas appropriées à tous les cas. C'est-à-dire qu'il pourrait être nécessaire de concevoir certaines dispositions spéciales en ce qui concerne les docu-

[Texte]

machine-readable form which do not exist for material which can be read and understood by human beings.

As far as trade secrecy goes, the Department of Justice, I believe, is looking into this issue. It would almost certainly involve consultation with the provinces. To the best of my understanding, nothing has happened there. I think, personally, that trade secrecy is a very valuable avenue to look into in terms of protection of information—not only in computerized form but in any form whatsoever. My understanding is that if governments did get into the issue of trade secrecy, they would look at it not only in the context of computerized information, but in the context of all information. Again, I think this would be a very valuable avenue to explore.

One of the features to note here is that not everything would be protected. My understanding is that the Department of Justice, to the extent that they would look at possible criminal sanctions, would perhaps want to tie those in with other rights which might exist in the civil law, whether they would be in copyright or in trade secrecy. You would not get into a situation where all information, regardless of how it was expressed, was protected by the criminal law.

There is a certain remote possibility, in terms of the Industrial Design Act, that—again, this would depend upon definitions; but at the present time, I think one can safely say that the Industrial Design Act has very, very few implications for the type of thing we are talking about.

Mr. Butler: On this last point, there is a gentleman called Roy Jackson who many years ago made a submission, I believe to the Ilsley Commission, on industrial property. This was back in the 1950s. It may have been the Economic Council; I am not sure. He advocated a short period of protection against all copy; I believe he said it should be three years.

It may seem that industrial design has nothing to do with it; but the rationale for industrial design protection is very similar, I think, to the rationale for protecting computer programs or data bases.

• 1205

As you realize, we are going through all the industrial property statutes, and when we get to industrial design, it may well be that the Industrial Design Act will be an appropriate place to deal with this kind of problem. You see, if you had a system which protected what I would call minor innovations, it would also protect innovations in the appearance of articles as well. So you could do the two in the same exercise.

The other place to look is the Trade Marks Act, Section 7. Under Section 7 there was a prohibition against unfair trade practices derived from the Paris Convention for the Protection of Industrial Property, and it ended with the catch-all phrase:

[Traduction]

ments assimilables par une machine qui n'existent pas pour les documents qu'un être humain peut lire et comprendre.

En ce qui concerne les secrets commerciaux, je crois que le ministère de la Justice est en train de s'intéresser à cette question. Il y aura presque certainement consultation avec les provinces. À ma connaissance, rien ne s'est encore passé de ce côté. Pour ma part, je pense que les secrets commerciaux représentent une voie très intéressante à explorer en matière de protection de l'information, qu'elle soit sous forme informatisée ou autre. Je crois comprendre que si les gouvernements se penchaient vraiment sur le problème des secrets commerciaux, ils l'examineraient non seulement dans le contexte de l'information informatisée, mais aussi dans le contexte de toute l'information. Je le répète, je pense que ce serait une voie très intéressante à explorer.

Il est à noter que tout ne serait pas protégé. Je crois comprendre que le ministère de la Justice, dans la mesure où il envisagerait des sanctions possibles pour les actes criminels, voudrait peut-être les associer à d'autres droits pouvant exister en droit civil, qu'il s'agisse des droits d'auteur ou des secrets commerciaux. On ne se trouverait pas dans une situation où toute information, de quelque façon qu'elle soit exprimée, serait protégée par le droit criminel.

En ce qui concerne la Loi sur les dessins industriels, il existe une très vague possibilité que, encore une fois, cela dépendrait des définitions, mais à l'heure actuelle, je pense qu'on peut affirmer que la Loi sur les dessins industriels a très, très peu de portée en ce qui touche le sujet qui nous intéresse.

M. Butler: En ce qui concerne ce dernier point, un homme du nom de Roy Jackson avait, il y a de nombreuses années, présenté un mémoire, je crois à la Commission Ilsley, sur la propriété industrielle. Cela remonte aux années 50. C'était peut-être au Conseil économique, je n'en suis pas sûr. Il préconisait une courte période de protection contre toute reproduction; je crois qu'il avait parlé d'une période de trois ans.

On pourrait croire que le dessin industriel n'a rien à voir là-dessus; mais la raison d'être de la protection du dessin industriel est analogue, je pense, à la raison d'être d'une protection des programmes et des bases de données informatiques.

Comme vous le voyez, nous étudions toutes les lois portant sur la propriété industrielle, et lorsque nous parlons de dessin industriel, il se peut fort bien que la Loi sur les dessins industriels soit celle qu'il conviendrait d'appliquer face à ce genre de problème. Voyez-vous, s'il y avait un système qui protégeait ce que j'appellerais des innovations mineures, ce système protégerait aussi les innovations dans l'aspect des articles. Il serait donc possible de faire les deux en même temps.

Il faudrait aussi consulter l'article 7 de la Loi sur les marques de commerce. En vertu de l'article 7, il y avait une interdiction de pratiques commerciales frauduleuses, découlant de la Convention d'union de Paris pour la protection de la

[Text]

"doing any other act contrary to honest commercial and industrial usage in Canada". For many years it was common for litigants to plead that section in trade secrecy cases.

The provision was found to be unconstitutional in the *Vapour & MacDonald* case..

Mr. Robinson (Etobicoke—Lakeshore): Because you were talking about morals instead of legal concepts.

Mr. Butler: I think the reason was that the section was drafted just too broadly. What is an industrial design? I believe an industrial design is a form of copyright, because if you look at the schedule of federal powers under the British North America Act, under the constitutional act it speaks of copyrights in the plural, and patents; it does not speak of trade marks. It seems to me we are legislating in relation to industrial design as a copyright.

Mr. Robinson (Etobicoke—Lakeshore): Do you gentlemen feel it is preferable to amend the present intellectual property acts that we have in Canada—there are several that you have mentioned—rather than have a special act on computer-based information or data-based information—information through computers? Do you feel it is better to amend what we have than to create a new act? Would your decision be based on the fact that if we just amend these acts, then the cases that have already been determined could still be relevant?

Mr. Butler: I would have to say I cannot answer that. Whether or not you should have a new statute is something which you people are experts at, rather than me. I am serious about that. I have observed the American process. The Americans have a new statute for every new subject. They do not seem to go back and amend statutes; they just create another one. I always thought that was a bad idea, but I am getting old now and I realize how hard it is to get legislation through. Sometimes I suspect it is easier to create a new law than it is to amend an old one.

Mr. Robinson (Etobicoke—Lakeshore): You, gentlemen, are talking about protection per se and not about penalties. In other words, we are not really talking about amending the Criminal Code, as far as you are concerned; we are talking about amending the statutes that we already have, the intellectual property statutes that can be helpful in preserving some property right or some propriety.

Mr. Butler: I think you have to amend the statutes, if for no other reason than that it is unclear now whether works in a non-human-readable form are protected. I will not go into all the details about that, but if you look at Section 3 of the present Copyright Act, it has a list of the various works which are protected and the exclusive right. What you will find is that when a work is translated or expressed in a different form, for instance when you take notations on a page—musical

[Translation]

propriété industrielle, qui se terminait par la phrase-clé: «faire un autre acte contraire aux honnêtes usages industriels ou commerciaux ayant cours au Canada». Pendant de nombreuses années, il était courant pour les plaideurs d'invoquer cet article dans les cas de secrets commerciaux.

La disposition a été jugée inconstitutionnelle dans l'affaire *Vapour and MacDonald*.

M. Robinson (Etobicoke—Lakeshore): Parce que vous parliez de principes moraux plutôt que juridiques.

M. Butler: J'estime que l'article avait été rédigé de façon trop large. S'agissait-il d'un dessin industriel? Je crois qu'un dessin industriel jouit d'une forme de droits d'auteur, parce que si vous étudiez la gamme des pouvoirs fédéraux conférés par la Loi de l'Amérique du Nord britannique, vous verrez qu'en vertu de la loi constitutionnelle, il est fait mention de droits d'auteur au pluriel, et de brevets; il n'est pas fait mention de marques de commerce. Il me semble que nous sommes en train de légiférer sur le dessin industriel en matière de droits d'auteur.

M. Robinson (Etobicoke—Lakeshore): Messieurs, croyez-vous qu'il est préférable de modifier les lois actuelles sur la propriété intellectuelle que nous avons au Canada (vous en avez mentionné plusieurs) plutôt que de passer une loi spéciale sur les données informatisées ou sur les données stockées dans les bases de données, c'est-à-dire l'information par ordinateur? Êtes-vous d'avis qu'il vaut mieux modifier les lois que nous avons plutôt que de créer une nouvelle loi? Votre décision serait-elle fondée sur le fait que si nous ne faisons que modifier ces lois, les cas qui ont déjà été réglés seraient toujours pertinents?

M. Butler: J'avoue que je ne puis répondre à cette question. Que nous adoptions ou non une nouvelle loi est une chose que vous, les experts, devez décider, plutôt que moi. Je suis très sérieux à ce sujet. J'ai observé le processus américain. Les Américains ont une nouvelle loi pour chaque nouveau sujet. Ils ne semblent pas regarder en arrière et modifier leurs lois; ils en créent une nouvelle. J'ai toujours cru que ce n'était pas une bonne idée, mais en vieillissant, je me rends compte combien il est difficile de faire adopter des lois. Parfois, je pense qu'il est plus facile de créer une nouvelle loi que d'en modifier une ancienne.

M. Robinson (Etobicoke—Lakeshore): Messieurs, vous parlez de protection en soi et non de pénalités. Autrement dit, nous ne parlons vraiment pas d'amender le Code criminel en ce qui vous concerne; nous parlons de modifier les lois que nous avons déjà, les lois sur la propriété intellectuelle pouvant aider à conserver certains droits de propriété ou certaines propriétés.

M. Butler: Je crois qu'il faut modifier les lois, ne serait-ce que parce qu'actuellement, il n'est pas clairement indiqué si des oeuvres présentées sous une forme que les humains ne peuvent lire sont protégées. Je n'entrerai pas dans tous les détails à ce sujet, mais si vous lisez l'article 3 de la présente loi sur les droits d'auteur, vous verrez qu'il comporte une liste des diverses oeuvres qui sont protégées et du droit exclusif. Vous constaterez que lorsqu'une oeuvre est traduite ou exprimée

[Texte]

notations—and you make a recording of that, it is an infringement to make the recording and it is an infringement to copy the recording.

Now, why would that be necessary if a computer program enjoyed copyright? Because, you see, if you think of the technology that is involved with a computer program, it is very similar to the exercise you go through in recording with what we call a sound recording.

• 1210

Going back to the example of the recipe, when you read the recipe in the book and you then bake the cake, you are doing what somebody does when they record the music.

So the point is nobody knows for sure whether these things are covered by copyright or not. This is a personal view on my part. I say they are not, because I cannot read them; I cannot see them. Since it is the judge who decides whether it is an infringement or not, if he cannot see it, then there is no infringement.

Mr. Robinson (Etobicoke—Lakeshore): Mr. Couchman, you referred to two different approaches, or two major approaches, in addressing the whole problem. One had to do with unauthorized access. The other I found rather intriguing. You talked about the extension of property rights and the extension of the concept of theft, and then you talked about an overlapping. I wonder if you would care to expand on that a bit. Is this by way of definition?

Mr. Couchman: What we were really trying to say in our submission is that from what we gather from various briefs and so on that we have seen and that have been presented to, say, the Department of Justice and so forth, these seem to be the two basic approaches. They do not overlap completely, because I think for example provisions on access would deal with things like mischief, which would not ever be related to copyright. For example, if someone gets into my data base and does something to it, or adds something to it, it would be very questionable whether that would ever be a violation of copyright, regardless of how it was defined, or whether that would be in any way an infringing act.

Now, conceivably there are certain other types of changes that might be infringements of copyright, but there are certain problems that could be dealt with by provisions relating to access or mischief and which could not be dealt with by property rights in the traditional sense. On the other hand, when you are simply dealing with the problem of copying something or making an adaptation of something, then you probably have alternative approaches that you could take. One is to grant some form of property protection, because property protection in the traditional sense—copyright deals not only with copying something, but also with making adaptations of it or making translations of it.

So if you simply want to protect the information as such to prevent copying of that information, then the property rights approach is one way of doing that. Obviously there are all sorts of other types of computer abuse which do not involve copying,

[Traduction]

sous une forme différente, par exemple lorsque vous prenez des notes sur une page (des notes musicales) et que vous les enregistrez, il s'agit d'une infraction à la loi et si vous copiez cet enregistrement, il s'agit aussi d'une infraction.

Pourquoi donc cela serait-il nécessaire si un programme d'ordinateur avait des droits d'auteur? Parce que, si vous me suivez bien, la technique d'un programme d'ordinateur est très semblable à celle que vous utilisez pour enregistrer une oeuvre avec un magnétophone.

Pour revenir à l'exemple de la recette, quand vous lisez la recette dans le livre avant de faire le gâteau, vous faites la même chose qu'une personne qui enregistre de la musique.

Donc, personne n'est bien sûr il peut être question de droit d'auteur pour ce genre de choses. C'est mon opinion personnelle. Selon moi, il ne peut pas en être question, parce que ce sont des choses qu'on ne peut pas lire, qu'on ne peut pas voir. Comme c'est le juge qui décide s'il y a violation, quand il ne peut rien voir, il n'y a donc aucune violation.

M. Robinson (Etobicoke—Lakeshore): M. Couchman, vous avez mentionné deux façons différentes ou deux principales façons d'aborder tout le problème. La première concerne l'accès non autorisé mais l'autre a piqué ma curiosité. Vous avez parlé de l'extension des droits de propriété et de l'extension du concept du vol, puis vous avez mentionné qu'il y avait un recoupement. Je me demande si vous pourriez nous donner un peu d'explications. Parlez-vous de la définition?

M. Couchman: En réalité, ce que j'essayais de dire dans mon exposé c'est que, d'après ce qu'il ressort des divers mémoires et autres documents que j'ai vus et qui ont été présentés, par exemple, au ministère de la Justice et à d'autres, ces deux solutions semblent être les deux principales. Elles ne se recoupent pas complètement, parce que je crois, par exemple, que les dispositions relatives à l'accès porteraient sur des choses comme les méfaits, ce qui n'a rien à voir avec le droit d'auteur. Par exemple, si quelqu'un a accès à ma base de données et modifie ou ajoute des données, je doute fort que ce soit considéré comme une violation du droit d'auteur, peu importe sa définition, ou comme un acte de transgression.

Il est concevable que certains autres types de modifications puissent constituer une violation du droit d'auteur, mais il y a certains problèmes auxquels s'appliqueraient les dispositions relatives à l'accès ou aux méfaits, mais non pas les dispositions touchant les droits de propriété, au sens traditionnel. D'autre part, lorsqu'il s'agit simplement d'empêcher qu'on copie quelque chose ou qu'on en fasse une adaptation, il y a probablement différentes façons de procéder. Tout d'abord, on peut prévoir une certaine forme de protection de la propriété au sens traditionnel; le droit d'auteur empêche non seulement de copier quelque chose, mais également d'en faire l'adaptation ou la traduction.

Donc, si vous voulez simplement protéger les données pour empêcher qu'on les copie, les droits de propriété sont une façon de le faire. Évidemment, il y a toutes sortes d'autres types de fraude par ordinateur qui ne comportent pas la copie de

[Text]

and those would be best dealt with by provisions relating to access. Our tentative feeling is that perhaps all problems with computer abuse could be dealt with through properly drafted access provisions, plus the various remedies that are available under intellectual property statutes. That is, it may not be necessary to create additional property rights in the Criminal Code beyond those which exist in the various intellectual property statutes.

Mr. Robinson (Etobicoke—Lakeshore): One further question, if I may. You talked about the limited period of protection from a life plus 50 years to a life plus 17 years, and so on, and I think you indicated that it could be quite a limited period of time. Do you have any rule of thumb as to how you determine the length of time there should be protection under each of these various acts that you mention? Or should they all be virtually the same? Or in a high-tech industry such as this, maybe the time limitation may be a year; something like that would be sufficient.

Mr. Couchman: In copyright protection, we are limited by our international treaty obligations. The protection there is basically fairly long. Probably the minimum period of protection we could grant to something in human-readable form would be the life of the creator plus 25 years. There are certain exceptions to that; for example photographs and sound recordings. But that is the basic minimum term that we are required by our intellectual property treaty obligations in the copyright area . . .

In general principle, the period should be the amount of time that enables the inventor or the creator to make a reasonable return on his investment. So if one were simply talking in terms of principle, one could say that the period of time for protection of a computer program should be the length of time it would enable someone to get a reasonable return on that investment.

Mr. Robinson (Etobicoke—Lakeshore): Maybe I could make one further intervention.

• 1215

I notice that from time to time you mention intellectual property, and then at other times you mention industrial property. Is there some commonality between the two, or are they mutually different? Maybe you would care to explain either their differences or their similarities.

Mr. Couchman: The term "intellectual property" can be used in two separate senses. There is the broadest sense, which includes all concepts, including industrial property. For example, when one refers to the World Intellectual Property Organization, one is using the term "intellectual property" in the broadest possible sense. The narrower meaning of that might be cultural property. Industrial property never includes copyright. When it is used, for example, in a law school or a curriculum, the term "industrial property" refers to things like

[Translation]

données, et la meilleure façon de s'y attaquer serait d'adapter des dispositions concernant l'accès. A première vue, je crois que tous les problèmes qu'entraînent les opérations informatiques frauduleuses pourraient être réglées par l'adoption de dispositions soigneusement rédigées concernant l'accès, en plus de l'application de toutes les mesures qu'autorisent les lois sur la propriété intellectuelle. Autrement dit, il n'est peut-être pas nécessaire d'ajouter dans le Code criminel d'autres droits de propriété à part ceux qui existent dans les diverses lois sur la propriété intellectuelle.

M. Robinson (Etobicoke—Lakeshore): Permettez-moi de poser une autre question. Vous avez mentionné la période de protection limitée allant d'une vie plus de 17 ans à une vie plus 50 ans et, ainsi de suite, et je crois que vous avez ajouté que ce pourrait être une période de temps très limitée. Avez-vous une règle empirique pour déterminer quelle période de protection devrait être prévue dans chacune de ces diverses lois dont vous parlez? Devraient-elles toutes être pratiquement les mêmes? Ou, dans une industrie de haute technologie comme celle-ci, la limite de temps pourrait peut-être être d'un an ou à peu près ce serait suffisant.

M. Couchman: Pour la protection du droit d'auteur, nous sommes limités par le traité international. Dans ce cas-là, la protection est assez longue. La période minimale de protection que nous pourrions accorder pour quelque chose d'humainement lisible serait probablement la durée de la vie de l'auteur, plus 25 ans. Cependant, il y a certaines exceptions: les photographies et les enregistrements sonores, par exemple. Mais, c'est la période minimale de base que nous sommes tenus d'accorder pour les droits d'auteur, à cause de nos obligations aux termes du traité sur la propriété intellectuelle.

En règle générale, la période en question devrait être le temps nécessaire pour permettre à l'inventeur ou à l'auteur de tirer un revenu raisonnable de son investissement. Par conséquent, si l'on parlait simplement de principes, on pourrait dire que la période de protection accordée pour un programme informatique devrait être la période nécessaire pour permettre à quelqu'un de tirer un revenu raisonnable de son investissement.

M. Robinson (Etobicoke—Lakeshore): Puis-je faire une autre intervention?

J'ai remarqué que vous parliez tantôt de propriété intellectuelle, tantôt de propriété industrielle. Y a-t-il un point commun entre ces deux notions ou sont-elles complètement différents? Peut-être pourriez-vous nous expliquer en quoi elles diffèrent ou en quoi elles se ressemblent.

M. Couchman: L'expression «propriété intellectuelle» peut avoir deux sens bien distincts. Elle peut par exemple être utilisée dans son sens large: elle recouvre alors toutes les notions, y compris celle de propriété industrielle. Ainsi, lorsqu'on parle de l'Organisation mondiale de la propriété intellectuelle, on donne à l'expression «propriété intellectuelle» son sens le plus large, le sens plus étroit pouvant se limiter à la propriété culturelle. La «propriété industrielle» ne désigne jamais le droit d'auteur. Utilisée dans une faculté de droit ou

[Texte]

patents and trade marks. Industrial property does not include copyright, which is more a type of cultural property or intellectual property in the narrow sense. But there is an overlap between the two, depending on how one uses the term "intellectual property".

Mr. Robinson (Etobicoke—Lakeshore): But then when you use the word "property" by itself, that is not sufficient; it must always be described. Would that be a fair statement?

Mr. Couchman: Right; because there is a real problem that would arise. If you simply use the term "property", a real problem would arise between the person who owned the physical object and the person who owned, say, the copyright in that object. For example, I may own a sound recording; I have the right to sell it, I have the right to rent it, but I do not have the right to duplicate it, I do not have the right to make a tape of that, because someone else owns the copyright in the work that is embodied in that sound recording. On the other hand, I can do an immense number of other things with it, because I own the object itself.

That is why it is necessary to draw a distinction between the ownership of the object, of the property, and the ownership of the intellectual property that is embodied in that object.

Mr. Robinson (Etobicoke—Lakeshore): Thank you very much.

The Chairman: Thank you, gentlemen, for your clarification. I think it was very helpful. We hope to see the new copyright law, or patent law . . . which one will come first?

Mr. Butler: I think you can look for a copyright law first. There are proposals for revisions of all the statutes in the works, including industrial design. We hope to publish a working paper in relation to industrial design relatively soon. There was a draft bill introduced into the Senate on trade marks I believe in 1978, or something like that. So all four of them are in the works.

The Chairman: But my understanding was that your department has been working very hard, bringing up to date these laws.

Mr. Butler: We feel like Sisyphus, pushing the rock up the hill and having it roll down on us.

The Chairman: This session I have some doubts, but I would be very interested, and in the next session we will be able to deal with these.

Mr. Butler: I was just going to make a point on industrial design and the short period of protection. One of the enormous problems is the participation of foreign rights owners in Canada. We are different from countries like the United States, where virtually everything is owned domestically. Here, for instance, in the patent system, 95% of the patents we grant go to people located abroad.

[Traduction]

dans un programme, elle désigne les brevets et les marques de commerce. Cette notion n'inclut cependant pas le droit d'auteur, qui est davantage un type de propriété culturelle, ou de propriété intellectuelle dans le sens restreint du terme. Mais il existe certainement un recoupement entre ces deux notions et elle varie selon le sens accordé à la «propriété intellectuelle».

M. Robinson (Etobicoke—Lakeshore): Il ne suffit donc alors pas de parler de «propriété»? Il faut toujours qualifier cette propriété. Est-ce bien cela?

M. Couchman: C'est exact; il faut toujours le faire, faute de quoi il y aura un vrai problème. En effet, si vous parlez simplement de «propriété», un conflit surgira entre le propriétaire de l'objet matériel et le propriétaire du droit d'auteur attaché à cet objet, par exemple. Supposons que je possède un enregistrement sonore: j'ai le droit de le vendre et de la louer, mais je n'ai pas le droit de le reproduire ni d'en faire une bande, parce que quelqu'un d'autre est propriétaire du droit d'auteur attaché à l'enregistrement sonore en question. Je peux par contre faire quantité d'autres choses puisque je possède l'objet lui-même.

Voilà pourquoi il est essentiel d'établir une distinction entre le fait de posséder un objet—la propriété—et celui de posséder le caractère intellectuel inhérent à cet objet.

M. Robinson (Etobicoke—Lakeshore): Je vous remercie beaucoup.

Le président: Je vous remercie, messieurs, d'avoir bien voulu apporter ces précisions. Je crois que cela a été très utile. Nous espérons qu'il y aura une nouvelle législation sur le droit d'auteur, ou sur les brevets. Laquelle verra le jour en premier?

M. Butler: Je crois que la législature sur le droit d'auteur sera la première. On étudie actuellement des propositions de révision de toutes les lois, y compris celles qui visent les dessins industriels. Nous espérons d'ailleurs publier bientôt un document de travail sur le dessin industriel. Un projet de loi sur les marques de commerce a été présenté au Sénat vers 1978, je crois. Les quatre sont donc à l'étude.

Le président: Je croyais que les gens de votre ministère avaient travaillé d'arrache-pied pour mettre ces lois à jour.

M. Butler: Nous avons l'impression, comme Sisvohe, d'être condamnés à pousser un rocher jusqu'au haut de la montagne et de le voir infailliblement rouler sur nous.

Le président: Pour cette session-ci, j'ai des doutes; mais j'aimerais vraiment traiter de ces questions à la prochaine session.

M. Butler: J'allais mentionner quelque chose au sujet du dessin industriel et de la courte période de protection. La participation des titulaires de droits étrangers au Canada constitue un très grave problème. La situation au Canada n'est pas la même qu'aux États-Unis, où presque tout appartient à des Américains. Prenons par exemple le système des brevets: 95 p. 100 des brevets accordés ici le sont à des gens qui vivent à l'extérieur du pays.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): I did not want to bring up the whole question of conflicts of law, because I assume they are just incredible, really.

Mr. Butler: But if you have a period of relatively short protection, what happens there is that most of your problems tend to disappear; the reason being that—say you run the period of protection from first publication. By the time non-Canadians market their goods in this country, the period of protection is nearly over. In any event, by the time they get an injunction against somebody it will be over. That is the reason why, as a practical matter, I favour short periods of protection, because all these enormous problems of domination by foreign interests of our economy just disappear under those circumstances. That is why I think you are heading in the right direction.

Mr. Robinson (Etobicoke—Lakeshore): In other words, we do not have to recreate the wheel; somebody else has already developed it and we will just use it.

Mr. Butler: That is another question... I am speaking personally now. I feel that what is really important in these issues is the terms of trade, because we are a trading nation. You can talk about all of this in isolation, as if there were no other countries in the world and Canada were the universe. You can do that in the United States, because for the Americans the United States is the universe; the world ends at the borders of the United States. Here it does not. Anything we do has to do with our trade relations with other countries.

• 1220

Mr. Robinson (Etobicoke—Lakeshore): I realize the Americans have a large domestic market and we do not.

Mr. Butler: That is right.

Mr. Robinson (Etobicoke—Lakeshore): But by the same token, the two countries are so intertwined industrially and so on that I would think anything that happens in the United States economically or otherwise affects Canada, and vice versa, because we are the largest trading partner the United States has.

Anyway, we do not want to get into that.

The Chairman: Thank you.

The meeting is adjourned.

[Translation]

M. Robinson (Etobicoke—Lakeshore): Je ne voulais pas aborder toute la question des contradictions entre les lois, parce que je trouve que c'est vraiment incroyable.

M. Butler: Mais si la période de protection est relativement courte, la plupart des problèmes ont tendance à disparaître, puisque vous dites, par exemple, que la période de protection commence au moment de la première publication. Lorsque les étrangers commencent à commercialiser leurs produits au pays, la période de protection est presque terminée. Quoi qu'il en soit, lorsqu'ils réussissent à obtenir une injonction contre quelqu'un, cette période est à coup sûr passée. Voilà pourquoi je suis en faveur de courtes périodes de protection, pour des raisons pratiques: tous les énormes problèmes de domination de notre pays par des intérêts étrangers se trouvent ainsi à disparaître. À mon avis, vous êtes donc dans la bonne direction.

M. Robinson (Etobicoke—Lakeshore): Autrement dit, nous n'avons pas à réinventer la roue; quelqu'un d'autre l'a fait, et nous n'avons qu'à l'utiliser.

M. Butler: Voilà une autre question. Je parle en mon nom propre maintenant. Je crois que ce qui compte vraiment ici, ce sont les conditions de commerce, parce que nous sommes une nation «commerciale». Vous pouvez aborder toutes ces questions dans un contexte d'isolement, comme s'il n'y avait aucun autre pays au monde et que le Canada était l'univers tout entier. Vous pouvez le faire aux États-Unis, parce que pour les Américains, l'univers se limite aux États-Unis: le monde finit à la frontière américaine. Ce n'est pas le cas au Canada. Tout ce que nous faisons porte sur les relations commerciales que nous entretenons avec les autres pays.

M. Robinson (Etobicoke—Lakeshore): Je sais que les Américains ont un très grand marché intérieur, que nous n'avons pas.

M. Butler: C'est vrai.

M. Robinson (Etobicoke—Lakeshore): Cependant, en même temps, les deux pays sont tellement liés industriellement et sur d'autres plans que je crois que tout ce qui se passe aux États-Unis, dans les secteurs économiques ou autres, touche le Canada et vice-versa, parce que nous sommes leur partenaire commercial le plus important.

De toute façon, nous ne voulons pas aborder ce sujet.

Le président: Merci.

La réunion est ajournée.





*If undelivered, return COVER ONLY to
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9*

*En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9*

WITNESSES—TÉMOINS

From the Department of Consumer and Corporate Affairs:

Mr. Tony Butler, Senior Policy advisor;

Mr. Bruce Cauchman, Policy advisor.

Du Ministère de la consommation et des corporations:

M. Tony Butler, Conseiller des politiques;

M. Bruce Cauchman, Conseiller des politiques.

HOUSE OF COMMONS

Issue No. 12

Wednesday, May 25, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 12

Le mercredi 25 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

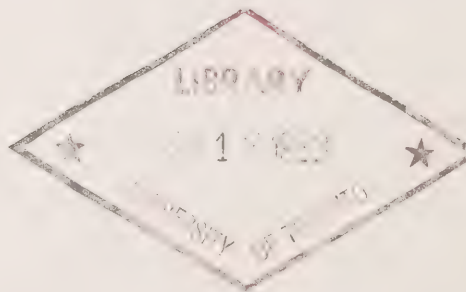
Questions relatives à l'ordre de renvoi

WITNESS:

(See back cover)

TÉMOIN:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, MAY 25, 1983
(14)

[Text]

The Sub-committee on computer crime met this day at 3:40 o'clock p.m., the Acting Chairman, Mr. Ken Robinson (*Etobicoke—Lakeshore*), presiding.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witness: From the Canadian Information Processing Society, Toronto: Mrs. Sally Woodhead, Chairman of Special Interest Group on Computer Security.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

The witness made a statement and answered questions.

At 4:43 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 25 MAI 1983
(14)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h40 sous la présidence de M. Ken Robinson (*Etobicoke—Lakeshore*), président suppléant.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoin: De la «Canadian Information Processing Society», Toronto: M^{me} Sally Woodhead, présidente, Groupe spécial d'intérêt sur la sécurité informatique.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Le témoin fait une déclaration et répond aux questions.

A 16h43, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by *Electronic Apparatus*)

[*Texte*]

Wednesday, May 25, 1983

• 1541

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I call the meeting to order.

The subcommittee resumes consideration of the order of reference before it respecting computer crime. We have before us today as a witness Mrs. Sally Woodhead, President of the Security Special Interest Group from the Canadian Information Processing Society.

Boy, that is really a mouthful. Since she is the witness for us today and is going to be making a statement, I wonder if she would at the outset explain what her group is all about, what it does and who is involved in the organization. It would probably save some questioning later on that aspect of it.

Mrs. Sally Woodhead (President, Security Special Interest Group, Canadian Information Processing Society): Okay. This year, CIPS, as we call it, has just turned 25 years old. The Canadian Information Processing Society was established to give people in the data processing industry a professional representation. Until that time, they had been a non-group, sort of a non-industry and non-professional, and this gave them more prestige. It gave them a forum; it gave them educational facilities, professional standing, etc.

Recently, the Canadian Information Processing Society has realized that the industry has been getting more and more specialized and harder to get a handle on. So instead of having this one large amorphous group, they have been starting these special interest groups, which we call SIGs for short, being nuts for acronyms. I am sure you are familiar with some of them. These have started to happen in the last three or four years.

CIPS has a total national membership of approximately 5,000 in Canada now. Toronto is the largest chapter, with almost 2,000. We now have approximately 14 SIGs in Toronto on various technical issues, including office automation and some very technical things.

The computer security group was one of the first ones to start up. We started with a core group of about 35 people in Toronto, who were professionally employed in this area and had a very keen interest. In the last three years, without a lot of advertising or pushing for new membership, it has grown to about 150 in Toronto, and groups have started up across the country. We now have four in operation and three in the planning stages, with a total national membership of several hundred, not including the Toronto group.

TÉMOIGNAGES

(*Enregistrement électronique*)

[*Traduction*]

Le mercredi 25 mai 1983

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): La séance est ouverte.

Le sous-comité reprend l'étude de son ordre de renvoi concernant le crime informatique. Nous accueillons aujourd'hui M^{me} Sally Woodhead, présidente du groupe spécial de la sécurité de l'Association canadienne de l'informatique.

Comme M^{me} Woodhead est notre témoin aujourd'hui et qu'elle fera une déclaration, elle pourrait peut-être d'abord nous expliquer en quoi consiste son groupe, ce qu'il fait et qui en fait partie. Cela nous évitera probablement des questions plus tard.

Mme Sally Woodhead (présidente, Groupe spécial de la sécurité, Association canadienne de l'informatique): Très bien. Cette année, l'ACI, comme nous l'appelons, célèbre son 25^e anniversaire. Elle a été établie pour représenter professionnellement l'industrie du traitement de l'information. Les gens qui travaillaient dans ce domaine n'appartenaient, jusqu'à ce moment-là, à aucun groupe, aucune sorte d'industrie ou de profession, et la société leur a donné plus de prestige. Ils ont maintenant une tribune, des installations d'enseignement, un statut professionnel, et ainsi de suite.

Dernièrement, l'ACI s'est rendu compte que l'industrie devenait de plus en plus spécialisée et de plus en plus difficile à suivre. Alors, plutôt que d'avoir un seul groupe, grand et amorphe, on a commencé à établir des groupes spéciaux, qu'on appelle GIP, ou SIG (*Special Interest Groups*), puisque nous sommes un peu maniaques des sigles. Je suis sûre que vous avez entendu parler de certains de ces groupes. Ils ont commencé à s'établir au cours des trois ou quatre dernières années.

L'ACI compte aujourd'hui approximativement 5,000 membres au Canada. La section la plus importante se trouve à Toronto, avec près de 2,000 membres. Nous avons environ 14 SIG, à Toronto, portant sur diverses questions techniques, y compris la bureautique et certaines techniques très spécialisées.

Le groupe de la sécurité des ordinateurs a été l'un des premiers à être créé. Tout a commencé avec un noyau d'environ 35 personnes, à Toronto, qui travaillaient dans le domaine de l'informatique et qui s'intéressaient énormément à la question. Au cours des trois dernières années, sans trop de publicité ou de campagne pour recruter de nouveaux membres, le groupe a accueilli environ 150 personnes, à Toronto, et d'autres groupes ont commencé à s'établir partout au pays. Actuellement, quatre groupes sont déjà actifs, et trois autres sont en train de s'établir, et le nombre de membres, à l'échelle nationale, s'élève à plusieurs centaines de personnes, excluant le groupe de Toronto.

[Texte]

There have been all kinds of bureaucratic moves in the association to try to make all these separate SIGs into one national one; but so far that has not worked, so we are all little separate pockets. The westerners have different ideas from the easterners in the case of most topics.

CIPS is primarily data processors, although that includes educators in the field, accountants and managers. But most of us are somehow employed in our day-to-day work with computers. The people in our SIG are employed in computer security, and therefore, have a vested interest in this specific topic we are addressing here today.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you very much for that introduction. I guess you can go ahead with your statement.

Mrs. Woodhead: Okay. The first couple of paragraphs are what I have just said, actually, so I will skip those.

We call ourselves EDP security officers. Now, actually, I should make one thing a little clearer. I am not myself an EDP security officer. I am not myself employed in any of the ways I am going to describe in this brief. I am serving as chairman of this group; and this is the main impetus of the group itself, not my own personal situation. I just want to make that clear at the beginning. I do not necessarily agree with everything in here, but my group does.

The membership of our group consists mainly of EDP security officers charged with the responsibility of computer security in large-sized organizations. While their companies typically realize . . .

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Perhaps you could slow down a little bit, because all this has to be translated. It is all being translated in that little booth behind you.

Mrs. Woodhead: Okay, sure.

• 1545

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So if you just slow down a little bit it will make it easier for them and it will be easier for us too; we will not have to think as fast.

Mrs. Woodhead: Sure.

The companies employing these EDP security officers typically do realize that some attention must be paid to the topic as evidenced by the fact that these people have their jobs in the first place. The emphasis on the topic is low.

Our membership is concerned, as they try to carry on with their jobs, that their senior management is under the impression that our current laws adequately cover any misdemeanours or abuse of the computer that might occur. Senior management is justifiably not terribly concerned, in the view of our group, as they do not see society or the law placing any

[Traduction]

Il y a eu toutes sortes de tentatives, au sein de l'association, pour regrouper tous ces SIG en un seul organisme national; mais, jusqu'à présent, cela n'a rien donné, et nous demeurons tous de petits groupes distincts. Les gens de l'Ouest ont des idées différentes de celles des gens de l'Est sur la plupart des sujets.

L'ACI regroupe principalement des informaticiens, et cela peut comprendre des enseignants, des comptables et des gestionnaires. Mais la plupart d'entre nous travaillent quotidiennement, d'une façon ou d'une autre, avec les ordinateurs. Les membres de notre groupe spécial (SIG) sont chargés de la sécurité des ordinateurs et, par conséquent, s'intéressent énormément au sujet que nous traitons ici aujourd'hui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci beaucoup pour cette introduction. Vous pouvez maintenant nous lire votre déclaration.

Mme Woodhead: Très bien. Je vais sauter les premiers paragraphes, puisque je viens de vous les résumer.

Nous nous appelons des agents de sécurité du traitement électronique des données. Mais je dois apporter une précision. Je ne suis pas, moi-même, agent de sécurité. Je ne remplis pas les fonctions que je vous décrirai dans mon mémoire. Je suis présidente du groupe, et l'exposé que je vais vous faire représente le point de vue du groupe, et non le mien. Je voulais apporter cette précision avant de commencer. Je ne suis pas nécessairement d'accord avec tout ce qui se trouve dans le mémoire, mais le groupe que je représente l'est.

Notre groupe est composé principalement d'agents de sécurité de l'informatique chargés de la sécurité des services informatiques dans de grandes organisations. Alors que les compagnies pour lesquelles ils travaillent se rendent bien compte . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Pourriez-vous ralentir un peu votre débit, parce que tout ce que vous dites doit être traduit. Il y a des interprètes dans la cabine derrière vous.

Mme Woodhead: Certainement.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Si vous pouvez ralentir un peu, cela facilitera la tâche des interprètes et la nôtre aussi; nous n'aurons pas à penser aussi vite.

Mme Woodhead: Très bien.

Les compagnies pour lesquelles travaillent ces agents de sécurité se rendent généralement compte qu'il faut accorder une certaine attention au sujet, la preuve en étant que les agents de sécurité sont déjà en poste. Mais l'intérêt est peu marqué.

Nos membres se soucient du fait que les cadres supérieurs ont l'impression que les lois présentement en vigueur recourent efficacement toute infraction ou utilisation abusive reliée à l'ordinateur susceptible de se produire. Notre groupe comprend que les cadres supérieurs ne s'intéressent pas tellement à la question, puisqu'ils n'envisagent pas que la

[Text]

importance on computer abuse as a specific issue, and therefore believe that our current theft, mischief, etc., laws can handle any abuse that may happen. However, when a company in a similar industry to that employing our security officers is hit by some computer abuse, and the story is splashed all over page 1, then there is a desperate scramble to make sure that the same thing "cannot happen here".

Our security practitioners, on the other hand, see not only the risks that may happen but also the lack of comment of society and the resulting combination; that resources can be lost with no tools available to either reclaim those resources or get your revenge, whatever you are looking for.

His job is a critical one, because on him, of course, rests not only the investment in the technology itself, but in many cases the means of carrying on business itself. He must therefore protect the physical and logical assets of the data processing department, which means not only the equipment but the programs and data within the equipment, and the people who work with it. He must examine every program and data file in that computer for criticality, timeliness, privacy, vulnerability. He must then analyse how much money he can spend to protect that.

There are many formulae for figuring out how much money you should spend to protect something, but none of them are foolproof and none of them necessarily work in all situations. So there is no simple answer to his problems; he has a very complex job.

He must also try to impress upon the users of his systems who should be accountable for what; who owns what programs; who owns what data; who owns the mailing list; who owns the payroll file; who should therefore be responsible for the security on that program. This gets very, very thorny, as I am sure you can well imagine. As it is right now, usually all responsibility rests on our security officer, which is obviously not a realistic situation, as I, as the payroll supervisor, can give away my password and totally screw up the whole system, and then the blame goes down to our little man trying desperately to protect everything.

It is also currently the case that if an employee is found abusing the computer system there are very few actions available to be taken. One of the few reasons, in our understanding of the way the law works today, that an employee can be fired without risk of wrongful dismissal suits is if a criminal act is involved. Our understanding of this is that it does not necessarily have to result in successful prosecution; that there just has to be a criminal act involved and you can therefore fire whether an employee contract exists or not. Very often today, to get rid of an employee who has abused your computer system, what you have to do to get rid of him is give him

[Translation]

société ou la loi accordent une importance particulière à l'utilisation abusive de l'ordinateur, et ont l'impression que les dispositions relatives au vol, au méfait, et ainsi des suite, des lois actuellement en vigueur sont suffisamment efficaces. Cependant, quand une compagnie du type qui fait appel à nos agents de sécurité est victime d'une infraction quelconque reliée à l'ordinateur, et quand l'incident fait la première page des journaux, alors là, la compagnie s'empresse de prendre les dispositions qui s'imposent pour que l'incident ne puisse se reproduire.

Par ailleurs, nos agents de sécurité connaissent non seulement les dangers inhérents à l'industrie, mais aussi les conséquences éventuelles du manque d'intérêt de la société; ils savent qu'on peut subir des pertes et qu'il n'existe aucun recours pour recouvrer les ressources perdues ou pour se venger, selon ce que vous souhaitez.

Le travail de l'agent de sécurité est primordial parce que c'est lui, évidemment, qui est chargé non seulement de protéger l'investissement technologique comme tel, mais dans bien des cas, d'assurer le fonctionnement de l'entreprise. Il doit donc protéger les biens physiques et logiciels du service de traitement des données, ce qui veut dire non seulement l'équipement, mais aussi les programmes et les données emmagasinés dans le système, et il doit en outre surveiller les employés. Il doit examiner chaque programme et chaque ensemble de données emmagasinées dans l'ordinateur, pour en établir l'importance, l'opportunité, le caractère privé et la vulnérabilité. Il doit ensuite déterminer combien d'argent il peut dépenser pour protéger cela.

Il y a de nombreuses formules pour calculer combien d'argent on peut dépenser pour protéger quelque chose; mais aucune formule n'est à tout épreuve ou ne peut fonctionner dans toutes les situations. Il n'y a donc pas de solution facile; le travail de l'agent de sécurité est très complexe.

Il doit aussi chercher à faire comprendre aux utilisateurs de ces systèmes qu'ils ont des responsabilités; il désigne les responsables de programmes, de données, de listes d'envoi, de dossiers de la paie; en fait, il détermine les responsabilités de chacun en ce qui concerne la sécurité d'un programme. C'est une tâche très délicate, comme vous pouvez bien vous l'imaginer, j'en suis sûre. Actuellement, toute la responsabilité repose sur l'agent de sécurité, et ce n'est pas vraiment réaliste, puisque moi, en tant que surveillante de la paie, je peux donner mon mot de passe et bouleverser complètement tout le système, et le blâme sera imputé à notre petit agent de sécurité qui tente désespérément de tout protéger.

En outre, il existe actuellement très peu de recours contre un employé qui utilise abusivement un système informatique. De la façon dont nous interprétons la loi aujourd'hui, l'un des rares motifs de renvoi d'un employé, sans que l'employeur s'expose à des poursuites, est la perpétration d'un acte criminel. D'après nous, cela ne veut pas nécessairement dire qu'il doit y avoir des poursuites judiciaires; le simple fait qu'il y ait infraction criminelle justifie le renvoi d'un employé, qu'il ait un contrat ou non. Très souvent, aujourd'hui, pour vous débarrasser d'un employé qui a utilisé abusivement votre système informatique, vous devez lui faire une bonne apprécia-

[Texte]

a good recommendation. Now this means he is going to go off and get a similar job somewhere else and probably carry on with his abuse. We may protect ourselves this way in our own companies, but we certainly do not protect the industry.

One of the keys to understanding some of the problems that our group, as employees of large corporations, faces are the kinds of people and kinds of expertise that he is working with. No one really understands what our computer security man is up to. Typically, corporate security are ex-policemen who do not understand technology. Internal audit, to a large extent, cannot keep up with technology. It is a mammoth job for anybody, particularly someone who is not dealing with it in their day-to-day job. Other data processors do not necessarily understand the risks that the company is facing and therefore the necessary safeguards that have to be put into place. Senior management does not understand why everything hinges on its computers when it worked so fine without them before. Why should it be any different now?

Even people fairly closely related to data processing departments currently feel that if someone steals something from their computer they are perfectly well protected by theft laws as they are today. When our computer security officers try to bring home to people that this is not the case and they use horror stories as examples, they are accused of being scaremongers.

• 1550

If the laws recognize, specifically, computer crime, we believe senior management would have their attention drawn to the seriousness of these issues and these computer security practitioners would have the law backing up their own technological expertise. Their organizations would recognize the need for everyone to share the responsibility for protection, as they do today when they lock up green ledger files to minimize the possibility of fraud.

I do not want to give the impression that these people desire these laws only to increase their budgets and ease their workloads. I have provided this background, in detail, of what their jobs are all about to show the closeness to, and understanding of, the issues and the competence to make recommendations. Laws are needed to make the role of the EDP security officer an effective one. These are the people who see close up what abuses do happen and can happen and what the results are. They have the most firsthand experience. They are the front line against computer abuse. But shaking a finger and slapping a wrist are not effective weapons for policing a potentially vast arena for computer abuse. These are the single group, probably more than any other, that sees the need for the change in the law and whose jobs will be most affected by these changes.

I have five points about what our membership would like to see in the way of any new laws. They do not want to see

[Traduction]

tion. Cela veut dire que l'employé peut obtenir un autre emploi ailleurs, et probablement continuer à faire ce qu'il faisait. C'est une façon, pour nous, de protéger nos compagnies, mais cela ne protège pas pour autant l'industrie.

Pour bien comprendre les problèmes que rencontrent les membres de notre groupe en tant qu'employés de grandes sociétés, il faut tenir compte d'un élément essentiel: soit le genre de personnes avec lesquelles nous travaillons et les spécialités du domaine. Personne ne comprend vraiment en quoi consiste le travail de nos agents de sécurité. De façon générale, la sécurité des sociétés est assurée par d'anciens agents de police qui ne comprennent pas la technologie. Les services de sécurité internes ne peuvent généralement pas suivre la technologie. C'est un travail colossal pour n'importe qui, particulièrement pour quelqu'un qui ne travaille pas dans le domaine. D'autres informaticiens ne comprennent pas nécessairement les risques auxquels s'expose la compagnie et ne connaissent pas les mesures de sécurité nécessaires qu'il faut mettre en place. Les cadres supérieurs ne comprennent pas pourquoi tout repose sur l'ordinateur, alors qu'on a pu s'en passer pendant si longtemps. Pourquoi la situation serait-elle différente maintenant?

Même des gens qui travaillent d'assez près avec les services informatiques estiment que les lois actuellement en vigueur concernant le vol les protègent assez bien contre toute infraction reliée aux ordinateurs. Quand nos agents de sécurité essaient de faire comprendre aux gens que ce n'est pas le cas et qu'ils donnent des exemples d'incidents vraiment horribles, on les accuse d'être alarmistes.

Si les lois reconnaissaient explicitement le crime informatique, nous estimons que les cadres supérieurs seraient sensibilisés à la gravité de la question et que les agents de sécurité auraient la loi pour les appuyer. Les compagnies reconnaîtraient que chacun doit assumer sa part de responsabilités pour protéger les systèmes informatiques, comme on ferme bien à clé, aujourd'hui, les classeurs, pour minimiser la possibilité de fraude.

Je ne veux pas vous donner l'impression que les agents de sécurité veulent ces lois uniquement pour que leur budget soit accru et que leurs charges de travail soient réduites. Je vous ai exposé en détail en quoi consiste leur travail, pour vous montrer leur appréciation et leur compréhension du problème et leur compétence à faire des recommandations. Il faut des lois pour que l'agent de sécurité puisse remplir son rôle efficacement. Il connaît très bien les abus qui peuvent se produire, et les conséquences qui en découlent. Il a une expérience des plus pertinentes. Il est au premier plan dans la lutte contre l'utilisation abusive de l'ordinateur. Mais les réprimandes ne sont pas un outil efficace de contrôle d'un domaine qui présente un si vaste potentiel d'abus. Le groupe des agents de sécurité est probablement celui qui, plus que tout autre, comprend le besoin de changer la loi, et dont le travail sera le plus touché par ces changements.

Nos membres ont fait cinq recommandations concernant toute nouvelle loi. Ils ne veulent pas que le terme «propriété»

[Text]

property redefined to include information—this being one of the thornier issues. I know some people argue very strongly that if we just redefined property the problem would be solved. In our opinion, this is a red herring with too many far reaching ramifications that we cannot foresee today. We would probably end up in a worse mess than the one we are in now. Also, the group feels that it does not bring home the fact that we are addressing, specifically, computer abuse. If you just tell the world at large that you are changing “property” to include various other intangibles, you are not really addressing computers as a specific issue.

The second recommendation is that specific offences be created, such as was done with theft of credit cards or theft of telecommunications. This is felt to be a cleaner, simpler method of approaching the problem and deals with the specific problem. Attention is then focused on the fact that we are addressing computer crime.

The third recommendation is that any legislation be worded extremely carefully so that it is not too tied to today's technology. Our technology is changing far too quickly for any law that is too specific to be effective for very long. I use the example here that “electromagnetic” should not be used in any definition of a computer, for example, because that is not going to be the case for very long.

The fourth recommendation is that the victim of any kind of computer abuse not be compelled by law to report that computer abuse. As was pointed out to us by an OPP officer at a meeting we had last month, if you did make it a crime not to report a crime, you would have so many crimes occurring out there that you would not be able to keep a handle on anything any more. The group feels that there should be leeway for internal action to be taken—for example, firing without prosecution and without good recommendations.

The fifth recommendation is a rather paranoid one and we realize that it may not be totally realistic and probably would be very difficult to enact. We would like to see some kind of responsibility, actually within the law itself, that companies have to make a defined minimum effort to protect themselves for the law protecting them to have any effect. This is along the lines of the Foreign Corrupt Practices Act in the States, where due care must be shown. This would mean that a company not taking proper security precautions would not be able to call in the protection of the law. We realize that this is a rather harsh sounding recommendation. At the very least, we would like to see onus taken at the time of sentencing, so that companies victimized in computer crimes realize that a large part of the responsibility must be theirs.

Because of their background, many of our members—who are, on the whole, not familiar with legal details, they are not lawyers—are not concerned with how the law is written, who writes it, what exactly it covers. The main issue, as far as they are concerned, is that the law recognized specifically that this is an area which can be abused and that this abuse is not

[Translation]

soit redéfini pour comprendre la notion d'information; ceci était l'une des questions les plus épineuses. Je sais que certains ont vraiment l'impression qu'une nouvelle définition du terme propriété résoudrait le problème. D'après nous, c'est beaucoup plus compliqué, et les conséquences d'une telle mesure sont beaucoup plus importantes que nous pouvons l'envisager aujourd'hui. Nous nous retrouverions probablement dans une situation encore pire qu'aujourd'hui. Le groupe estime en outre qu'une nouvelle définition de ce terme ne réglerait pas le problème qui nous occupe: l'utilisation abusive de l'ordinateur. Si vous dites simplement que vous changez la définition de «propriété» pour qu'elle englobe toutes sortes d'éléments intangibles, vous ne parlez pas explicitement d'ordinateurs.

La deuxième recommandation propose de créer des infractions précises, comme on l'a fait pour le vol des cartes de crédit ou le vol dans le domaine des télécommunications. On estime que c'est un moyen plus clair et plus simple d'aborder le problème et de le résoudre. L'attention porterait ainsi sur le crime informatique.

La troisième recommandation porte sur le libellé de la loi, et on demande qu'il ne soit pas trop lié à la technologie d'aujourd'hui. Notre technologie évolue beaucoup trop rapidement, et aucune loi trop précise ne peut être efficace pendant très longtemps. Il ne faudrait pas parler, par exemple, d'électromagnétique dans la définition de l'ordinateur, parce que cela va changer d'ici peu.

La quatrième recommandation est que la victime de toute infraction reliée à l'ordinateur ne soit pas tenue par la loi de signaler l'infraction. Comme nous le faisait remarquer un agent de la Sûreté provinciale de l'Ontario lors d'une réunion, le mois dernier, si c'était un crime de ne pas signaler une infraction, le nombre de crimes serait tellement élevé qu'on ne saurait où donner de la tête. Le groupe estime que la compagnie devrait disposer d'une plus grande marge de manoeuvre pour pouvoir congédier quelqu'un sans aucune forme de procès, ni appréciation favorable.

La cinquième recommandation reflète une certaine paranoïa, et nous nous rendons bien compte qu'elle n'est peut-être pas très réaliste et qu'elle serait probablement très difficile à appliquer. Nous aimerions que la loi définisse des normes minimales de sécurité auxquelles seraient assujetties les compagnies pour avoir droit à la protection que la loi vise à leur donner. Cela correspond à la loi américaine dite *Foreign Corrupt Practices Act*, qui oblige les compagnies à prendre certaines précautions. Cela veut dire qu'une compagnie qui ne prendrait pas les précautions voulues ne pourrait faire appel à la loi. Nous reconnaissons que c'est une recommandation plutôt dure. Tout au moins, nous aimerions que les compagnies victimes de crimes informatiques assument une partie du blâme au moment du prononcé de la sentence, pour qu'elles prennent conscience de leurs responsabilités.

A cause de leur expérience, beaucoup de nos membres, qui, de façon générale, ne connaissent pas les détails légaux, n'étant pas juristes, ne se préoccupent pas de savoir comment la loi est rédigée, qui la rédige et ce qu'elle comprend exactement. Ce qui importe pour eux, c'est que la loi reconnaisse explicitement qu'il s'agit d'un domaine où des abus peuvent se produire, et

[Texte]

acceptable. Our group would like the law to serve primarily as a deterrent and as a statement of what is ethical. In the final analysis, the perpetrators should be punishable.

• 1555

In fact, many computer crimes are technologically preventable. We, as computer security officers, know that. But only if the law supports us do we think others will take seriously the commitment that must be made to protect in an industry where technological advances are made and implemented before society has had a chance to understand and react.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you, Mrs. Woodhead, for your statement. I think Mr. Beatty wishes to ask a few questions first.

Mr. Beatty: Thank you, Mr. Chairman. Thank you, Mrs. Woodhead, for what I think is a very useful presentation. I think you have highlighted some of the key points the subcommittee will have to look at. I will preface my first question by saying that, as a result of the hearings, my views are evolving in the direction you outlined, including particularly as it related to property, and whether or not we should be redefining property to include information. Also I am inclining towards the belief that perhaps what we should do is to create a crime of data trespass or computer trespass; that the issue would be unauthorized access to computer facilities. I am wondering whether that would satisfy your concern; whether you feel that might be the neatest and cleanest way of closing the loophole.

Mrs. Woodhead: I think that addresses exactly what this group is trying to highlight here; that by redefining property . . . well, here I might add that we have a fairly large membership in our group of police of various forces, and they think, almost unanimously, that by redefining property, their problems are solved. The majority of our group, being these EDP security officers, feel very strongly—we have great arguments about it—that if you do just redefine property and use the laws that already exist for theft of property and mischief to property, etc., you are not going to see the whole picture for a long time to come, and you are going to run into incredible problems five years from now. Examples were given in espionage cases where property gets all very technical and the question is asked as to how do you define it, etc. It is too pat and far too . . . it is changing the focus of the way the laws were written in the first place. The laws were written to deal with specific events at the time and, by trying to take those same laws and reinterpret them to fit today, we will make very many complications. We will make peoples' lives very complicated.

Mr. Beatty: In specific cases such as espionage where you are dealing with official secrets, or in cases where trade secrets or where copyright is involved, presumably these are forms of intellectual property and which the law does recognize as property; there is a well established tradition there. The

[Traduction]

que les abus sont condamnables. Notre groupe aimerait que la loi ait d'abord un effet de dissuasion et qu'elle expose ce qui est acceptable. En dernière analyse, les auteurs d'infractions devraient être punis.

En fait, il est possible de prévenir technologiquement de nombreux crimes informatiques. Nous, en tant qu'agents de sécurité, le savons. Mais nous estimons que ce n'est qu'avec l'appui de la loi que nous réussirons à faire comprendre aux autres l'importance de s'engager pour protéger une industrie où les progrès technologiques sont tellement rapides que la société n'a pas le temps de les comprendre et de réagir.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci, madame Woodhead, pour votre déclaration. Je pense que M. Beatty a quelques questions à vous poser.

M. Beatty: Merci, monsieur le président. Merci, madame Woodhead, pour votre exposé très utile. Je pense que vous avez fait ressortir certains points clés sur lesquels devra se pencher le sous-comité. En guise de préface à ma première question, je dirais que, par suite des audiences du Comité, mes idées ont évolué dans le sens de votre exposé, particulièrement en ce qui concerne la propriété et la question de savoir si la définition de ce terme devrait comprendre la notion d'information. Je suis en outre de plus en plus favorable à l'idée que nous devrions créer une infraction de violation d'information ou d'ordinateur; c'est-à-dire que nous devrions insister sur l'accès non autorisé à des installations d'ordinateur. Trouveriez-vous cela satisfaisant? Pensez-vous que ce serait la meilleure façon de boucler la boucle?

Mme Woodhead: Je pense que vous touchez exactement à ce que le groupe tente de faire ressortir ici; c'est-à-dire qu'une nouvelle définition de propriété . . . Je pense que je devrais dire que notre groupe est constitué en assez grande partie d'agents de police de différents services, et qu'ils croient presque tous qu'une nouvelle définition de propriété réglerait tous leurs problèmes. La majorité des membres de notre groupe, qui est composé d'agents de sécurité des systèmes de traitement des données, sont très catégoriques: nous avons beaucoup d'arguments contre une simple redéfinition de «propriété» et le recours aux lois existantes pour les questions de vol et de méfait en matière de propriété, car vous n'aurez toujours pas abordé l'ensemble du problème, ce qui vous causera énormément d'ennuis d'ici à cinq ans. On a donné des exemples de cas d'espionnage où la notion de propriété est très technique, et on se pose la question de savoir comment la définir, et ainsi de suite. Si la définition est trop rigide et trop . . . Cela change l'esprit dans lequel les lois ont été rédigées originalement. Les lois ont été écrites pour traiter d'incidents particuliers à l'époque, et en essayant d'adapter ces mêmes lois à la situation d'aujourd'hui, nous nous créons de nombreux problèmes. Nous compliquerons énormément la vie des gens.

M. Beatty: Dans des cas particuliers comme l'espionnage, où il est question de secrets officiels, ou dans les cas de secrets industriels ou de droits d'auteur, il s'agit sans doute là de certaines formes de propriété intellectuelle reconnues par la loi; la tradition est bien établie. Le problème, c'est d'étendre la

[Text]

problem comes in extending those concepts more broadly and, in particular, that you would create an asymmetrical relationship between manually-stored information and electronically-stored information—one might be defined as property and not the other. The advantage that I can see to data trespass or computer trespass laws is that you have something then analogous to what happens if you are breaking into a person's office or into his filing cabinet to get at information.

Mrs. Woodhead: Break and enter has been suggested. Trespass has been suggested. Those are all, we feel, much more appropriate solutions than to try to redefine a law which was meant to protect your physical property, and which is valid for protecting your physical property.

Mr. Beatty: Could I pick up on your point No.5? You are somewhat ambiguous about it yourself. I am wondering whether at this point it is not premature to argue that the government should be putting data security standards on institutions because it is a relatively new area and very difficult, I would think, to establish adequate definition. We do not, in other cases of theft, put that sort of onus on the potential victim of the crime—you know, that your silverware must be properly locked away and you must have a proper lock on the front door and perhaps a guard dog or something else. I am not sure that perhaps in the short term the best way to deal with that might be through the marketplace which may, to an extent, solve the problem itself. That is, if an institution is victimized and does suffer serious losses as a result of computer crime, it will find that it is cost-effective to put proper security measures in place, that it is a good investment of manpower and of resources.

• 1600

Secondly, it may be that the insurance industry may want to take a look at this as well, and determine what is the condition of contract for insuring companies against losses. They might not want to require that the institution have proper data security standards.

Mrs. Woodhead: Three points on that: the first one is that there is an analogy in current law to this kind of onus placed on the owner of an asset in the Gun Control Act, where, if you do not protect your guns properly and they are stolen, you are responsible for part of the crime that is committed with those guns.

Mr. Beatty: The reason for that was to prevent damaged innocent third parties from the firearm, once it gets into the hands of the criminal.

Mrs. Woodhead: That is not clear in the law though. We still have an onus on the owner of the gun.

Mr. Beatty: Yes, but that was the purpose for it at the time. That is why it is not written into theft law across the board. In this instance, the government felt that firearms were sufficiently dangerous that, if they were to get loose and into the hands of criminals, third parties could be injured. I could see that an argument could be made, that where data that related to a third party was stored in an institution's computer,

[Translation]

portée de ces principes, et en particulier de créer des rapports asymétriques entre de l'information emmagasinée manuellement et de l'information emmagasinée électroniquement; dans un cas, il s'agit de propriété et dans l'autre, non. L'avantage que je vois dans des lois concernant la violation d'information ou d'ordinateur, c'est qu'on a une infraction analogue à l'entrée par effraction dans le bureau de quelqu'un, ou au vol de renseignements conservés dans un classeur.

Mme Woodhead: On a parlé d'entrée par effraction. On a parlé de violation. D'après nous, ce sont toutes des solutions beaucoup plus efficaces qu'une nouvelle définition de «propriété» dans la loi qui est destinée à protéger la propriété physique et qui est efficace pour cela.

M. Beatty: J'aimerais vous parler de votre cinquième recommandation. Vous semblez un peu incertaine vous-même. Ne pensez-vous pas qu'il est un peu prématuré de dire que le gouvernement devrait imposer aux institutions des normes de sécurité de l'information, étant donné que c'est un domaine relativement nouveau et qu'il serait très difficile, je pense, d'établir une définition efficace. Je ne crois pas qu'on impose ce genre de responsabilité aux victimes éventuelles d'autres genres de vols; on ne demande pas que votre argenterie soit mise sous clé, ou que votre porte soit munie d'un bon verrou, ou que vous ayez un chien de garde, ou quoi que ce soit. Je ne suis pas sûr qu'à court terme, la solution à ce problème ne doive pas venir du marché lui-même. En effet, si une institution est touchée et subit des pertes par suite d'un crime relié à l'informatique, elle jugera rentable d'instaurer des mesures de sécurité adéquates. Elle voudra y affecter du personnel et des ressources.

Par ailleurs, il se peut que les compagnies d'assurances examinent la situation et déterminent certaines conditions pour la protection des entreprises contre les pertes. Et il se peut qu'elles n'obligent pas les entreprises ou les institutions à avoir des normes de sécurité appropriées pour les données.

Mme Woodhead: Je voudrais dire trois choses à ce sujet. D'abord, il y a quelque chose dans la législation actuelle pour ce qui est du fardeau imposé au propriétaire d'un bien. En vertu de la Loi sur le contrôle des armes à feu, si quelqu'un ne protège pas adéquatement ses armes à feu ou qu'elles sont volées, il peut être tenu partiellement responsable des crimes commis avec ses armes à feu.

M. Beatty: Dans ce cas, il s'agissait de protéger les tierces parties innocentes de l'usage des armes à feu, une fois qu'elles tombaient aux mains de criminels.

Mme Woodhead: Ce n'est pas si clair dans la loi. Il reste que le fardeau est imposé au propriétaire de l'arme à feu.

M. Beatty: Dans ce cas, c'était l'intention. C'est pourquoi cette disposition ne s'applique pas ailleurs dans la législation sur le vol. Dans ce cas précis, le gouvernement a jugé que les armes à feu étaient suffisamment dangereuses, si elles tombaient aux mains d'éléments criminels, pour que des tierces parties en souffrent. On pourrait toujours faire valoir que lorsque des données touchant une tierce partie, par exemple,

[Texte]

perhaps there should be some data standards involved there—for example, for your medical record or credit record, or employment record and so on.

Mrs. Woodhead: Anyway, I just wanted to bring out that there is an analogy in current law.

Mr. Beatty: It is not unheard of.

Mrs. Woodhead: Right. The second thing... I wanted to address your last point first about insurance companies. I do not know if you are familiar with the Lloyds of London new risk analysis package that is available. It is the first package available in the world that will protect you from someone destroying your data base; stealing your customer master file, etc. But it is so phenomenally expensive... I think one of the banks, which is a member of our group, figured out that they would have to have a provable—under very strict guidelines laid down in the policy... \$10 million computer crime every five years to pay for the policy itself. That is not cost-effective insurance.

It is going to be a long time before the insurance industry can deal with this kind of thing: how do you value information? It is definitely an alternative, but it will be a long time coming. The main point is that the industry itself should be—as I say in the very last paragraph, we can technologically prevent a lot of the computer crimes that do happen today. What we need is a higher awareness on the part of people who use computers to run their businesses that they do face these risks.

Now, the press is helping us tremendously in this by splashing the stories on page 1 when they do happen. But again, it is a very slow process. CIPS is working very hard at a certification accreditation process similar to what a chartered accountant might go through so that they can police themselves to a certain extent. If you are a member of CIPS, you are an ethical, loyal data processor. If you do perpetrate something which is against the code of ethics of policy of CIPS as an organization, and then you lose your membership, you are no longer a data processor in good standing.

We have been working at this too for a long time, but it requires getting all the universities to agree on certain curricula requirements. It requires international liaison with affiliated groups in other countries, but it is going to happen. By joining CIPS you will sign codes of ethics, you will pledge yourself to be a member in good standing with the society and uphold the laws, etc.

When this becomes the case, we will have a lot more control over the data processing departments of any company, and that includes the company that does not really realize that his computer is running the business for him and is going to be absolutely up the creek if someone steals his next tender, and does not realize it today. But if we have these ethical data processors in there who are protecting it for him... This also goes for software protection. The industry is protecting itself there by making software packages and micro-computers

[Traduction]

un dossier médical, un dossier de crédit, d'emploi, et le reste, se trouvent dans l'ordinateur d'une institution, il devrait y avoir des normes quelconques.

Mme Woodhead: Je voulais simplement vous faire remarquer qu'il y avait quelque chose de semblable dans la loi actuelle.

M. Beatty: Je sais que ce n'est pas nouveau.

Mme Woodhead: Votre dernier point avait trait aux compagnies d'assurances. Je ne sais pas si vous connaissez la nouvelle offre d'analyse des risques de la *Lloyds*, de Londres. C'est la première assurance au monde qui peut vous protéger contre la destruction de vos données, le vol de votre fichier principal sur vos clients, et le reste. Son coût est cependant extrêmement élevé. Je pense que l'une des banques qui fait partie de notre groupe a établi qu'en vertu des conditions très strictes de la police, il lui faudrait être victime d'un crime relié aux ordinateurs, prouvable, d'une valeur de 10 millions de dollars, tous les cinq ans, pour en arriver à faire ses frais. Ce n'est pas une assurance très rentable.

Il faudrait beaucoup de temps pour que les compagnies d'assurances parviennent à s'adapter. Quelle est la valeur de l'information? C'est une possibilité, mais elle risque de mettre beaucoup de temps à se réaliser. Il faut que l'industrie elle-même fasse quelque chose d'abord. Comme je le dis dans le dernier paragraphe de mon mémoire, beaucoup de crimes reliés aux ordinateurs peuvent être évités actuellement, grâce à la technologie. Il faut simplement que les utilisateurs des ordinateurs prennent davantage conscience du fait qu'ils courent des risques dans la conduite de leurs affaires.

La presse nous aide beaucoup à cet égard en faisant de ces incidents ses manchettes. Mais le processus est quand même lent. L'ACI fait des efforts considérables en vue d'instaurer un système d'accréditation semblable à celui qui s'applique aux comptables agréés, de façon à ce qu'il y ait une autosurveillance quelconque. Si vous appartenez à l'ACI, vous devez vous comporter de façon professionnelle et loyale en matière d'informatique. Si vous allez à l'encontre du code de déontologie ou de la politique de l'ACI en tant qu'organisme, vous n'êtes plus membre et vous n'êtes plus considéré comme un informaticien en règle.

Nous y travaillons depuis longtemps, mais il faudrait que toutes les universités s'entendent sur un certain nombre de conditions préalables. Il faut également une liaison avec les groupes affiliés des autres pays, mais c'est possible. En devenant membre de l'ACI, vous vous engagez à respecter un certain code de déontologie, vous vous engagez à être un membre en règle et à respecter les lois, et le reste.

Lorsque nous aurons finalement mis en place le système, nous pourrions avoir un meilleur contrôle sur les services informatiques des compagnies, y compris les compagnies qui ne savent pas que ce sont les ordinateurs qui dirigent leurs affaires et qu'elles risquent la désorganisation la plus complète si jamais quelqu'un met la main sur leur prochaine soumission, par exemple, sans qu'elles s'en aperçoivent. Avec des informaticiens professionnels qui se chargent de les protéger... Tout cela fait partie de la protection du logiciel. L'industrie elle-

[Text]

cheap enough that everybody can afford them: so what is the point of stealing it?; providing extra support reference capacities: if you do buy from us instead of stealing from your next-door neighbour you will get these extra updates, you will get these extra newsletters, this kind of thing—and it has been very effective so far.

• 1605

So I think the industry is trying to take steps, but they are not going to be able to do it all by themselves.

Mr. Beatty: I accept that. I think the steps that you are referring to in terms of a code of standards by CIPS, which would make it more of a professional organization with a profession code of conduct, are useful, although I suppose in the example that you cited where in some instances the only way to get rid of a bad employee is to give him a good recommendation it is hard to see how CIPS could step in where the institution refuses to prosecute or refuses to put a black mark on the individual's record.

Mrs. Woodhead: Again, what we need there is a much more aware society so we do not have to give these people these recommendations. If everybody understands the risks and therefore realizes that what this person did is not an acceptable thing, whether it is illegal or not, then he is not going to win his wrongful dismissal suit and he is not going to get anything from anybody, and we do not have to trade anything in that case.

Mr. Beatty: Thank you. I think it is an excellent brief. In both your responses and your brief there was such clarity that I have no further questions.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you, Mr. Beatty. I will ask a few.

First of all, Mrs. Woodhead, do you organize provincially or do you just organize generally?

Mrs. Woodhead: Well, both. Do you mean our SIG itself?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes.

Mrs. Woodhead: At the same time we set up our Toronto group a fellow here in Ottawa set up a "national" group. Now, Ottawa is not the best place for a national group of this sort because most of the data processors in Ottawa are government employees, they do not represent the industry of the country and there are not that many of them here. So we by default became the national group in Toronto. We have taken the responsibility of helping the other groups in the other provinces organize—how they should set up their programs, this kind of thing—but we are not officially connected.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Would it be fair to say that you really organize

[Translation]

même se protège en produisant des paquets programmes et des micro-ordinateurs suffisamment peu coûteux pour qu'ils soient à la portée de tout le monde. À ce moment-là, pourquoi les voler? Il y a également les références supplémentaires. Si vous achetez de telle ou telle compagnie plutôt que de voler chez votre voisin, vous avez droit à des révisions, à des bulletins d'information, à toutes sortes d'avantages supplémentaires. Cette méthode a eu beaucoup de succès.

L'industrie, donc, est prête à faire sa part, mais elle ne peut pas tout faire seule.

M. Beatty: Je le comprends. Je pense que votre idée d'un code de déontologie à l'intérieur de l'ACI est excellente; elle deviendrait à ce moment-là une association professionnelle. Cependant, vous avez dit vous-même que dans certains cas, la seule façon de se débarrasser d'un mauvais employé est de lui donner de bonnes recommandations. Il est difficile d'envisager une intervention quelconque de la part de l'ACI lorsqu'une institution refuserait d'intenter des poursuites contre quelqu'un, refuserait de lui donner une mauvaise note dans son dossier.

Mme Woodhead: Il faut que la société, de façon générale, soit mieux informée, de façon à ce que ces gens ne reçoivent pas de bonnes recommandations. Si tout le monde est au courant des risques et que ces gens ont commis une faute inacceptable, que ce soit illégal ou non, il est peu probable qu'ils puissent gagner leur cause pour renvoi sans motif valable et obtiennent un montant quelconque. À ce moment-là, nous n'avons pas à accepter de compromis.

M. Beatty: Merci. Je pense que votre mémoire est excellent. Vous avez été tellement claire dans votre mémoire et dans vos réponses que je n'ai plus de questions.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci, monsieur Beatty. J'ai quelques questions à poser au témoin.

D'abord, madame Woodhead, est-ce que vous vous organisez sur une base provinciale, ou simplement générale?

Mme Woodhead: Les deux. Vous parlez du groupe d'intérêt particulier?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui.

Mme Woodhead: Au moment où nous organisons notre groupe de Toronto, quelqu'un ici, à Ottawa, mettait sur pied un groupe dit «national». Il se trouve qu'Ottawa n'est pas l'endroit le mieux indiqué pour un groupe national, parce que la plupart des informaticiens ici, à Ottawa, sont à l'emploi du gouvernement. Ils ne représentent pas l'industrie du pays; de toute façon, ils ne sont pas si nombreux. C'est ainsi que, par nécessité, nous sommes devenus, à Toronto, le groupe national. Nous avons pris l'initiative d'aider les groupes des autres provinces à se constituer, à établir leurs programmes, etc. Cependant, nous n'avons pas de liens officiels avec eux.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous organisez des groupes là où vous constatez

[Texte]

where there seems to be a general interest in most of the major cities where there is data processing?

Mrs. Woodhead: Yes. Specifically, we have organized in Calgary, where all our oil companies are and there is an awful lot to protect; we have organized in Toronto, where all the major banks are headquartered, except for one or two, who still have large data processing centres there; we have organized in Vancouver just recently, where we have a lot of trade and export organizations and natural resource organizations with large data processing departments; and we have organized in Montreal.

The other cities that are thinking about it are Halifax and Winnipeg... I forget the last one, but they are all major corporate headquarters.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mainly the larger cities where they have large head offices, I suppose—provincial head offices or Canadian head offices? Those were the ones?

Mrs. Woodhead: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Have you considered broadening it even further and getting people in most of the cities and towns of Canada involved in this kind of program? Really, I should get your opinion rather than tell you what I think, but it just seems to me from what you are doing that if you are trying to make people in the business, so to speak, aware of what is going on and what to look out for and so on you should have full-time organizing in effect right across the country.

Mrs. Woodhead: We would like very much to do that. Unfortunately, all of us who serve in any kind of executive capacity in these groups hold down full-time jobs. We volunteer our time, our own computers for our mailing lists, our own stamp machines, etc. It has been very difficult to get commitment from people to take on these responsibilities. We do have members at large, so to speak, from all over Canada, including a few in the Northwest Territories, in the special interest group.

So the problem is getting any kind of budget to disseminate information, which is what we really want to do. We want any story that happens and makes it to the Vancouver newspaper known by the guy who is also in Moncton, New Brunswick, but it is very difficult to do that at this stage. We are hoping that as we grow we will have more resources available to us.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you belong to the Consumers' Association of Canada?

• 1610

Mrs. Woodhead: No, although I am sure you are aware that in March we had a consultative session with the Department of Justice, with various members of the data processing industry,

[Traduction]

un intérêt quelconque, c'est-à-dire dans la plupart des grandes villes où il y a beaucoup de systèmes informatiques.

Mme Woodhead: Oui. Nous avons un groupe à Calgary, où beaucoup de compagnies pétrolières sont installées et où il y a beaucoup à protéger. Nous avons un autre groupe à Toronto, où se trouvent les sièges sociaux des grandes banques, à l'exception d'un ou deux. Il y a là de très importants centres d'informatique. Nous avons également établi, il y a quelque temps, un groupe à Vancouver, où il y a beaucoup d'organismes de commerce à l'exportation, d'organismes voués aux ressources naturelles également. Ils comptent tous d'importants services informatiques. Nous avons enfin un groupe à Montréal.

Il y a encore Halifax, Winnipeg, et une autre ville, dont j'ai oublié le nom pour l'instant, qui y songent sérieusement. Ce sont toutes des villes où sont établis d'importants sièges sociaux.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je suppose que ce sont toutes des villes où il y a des sièges sociaux, des bureaux provinciaux et des bureaux nationaux.

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Avez-vous envisagé d'étendre vos activités encore davantage et d'inclure les gens intéressés à ce genre de programme dans la plupart des villes du Canada? Je ne peux pas vous dire quoi faire, mais il me semble que si vous voulez vraiment alerter les hommes d'affaires à ces problèmes et leur dire quoi surveiller, vous devriez mettre sur pied des groupes dans tout le pays.

Mme Woodhead: Nous voudrions bien avoir l'occasion de le faire. Malheureusement, nous avons tous, nous qui sommes à la tête de ces groupes, des emplois à temps plein. Nous sommes des bénévoles, nous utilisons nos propres ordinateurs, nos propres listes d'adresses, nos propres machines à affranchir, etc. Il est très difficile de recruter des gens qui seraient prêts à assumer de telles responsabilités. Remarquez que dans le groupe d'intérêt particulier nous avons des gens de tout le Canada, y compris des gens des Territoires du Nord-Ouest.

Ce que nous voudrions, c'est avoir un budget pour pouvoir diffuser de l'information. Nous voulons que ce qui se passe à Vancouver et fait la manchette des journaux, à Vancouver, soit connu des gens de Moncton, au Nouveau-Brunswick. Nous avons bien du mal pour l'instant. Nous espérons qu'au fur et à mesure que nous prendrons de l'expansion, nous aurons davantage de ressources.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous faites partie de l'Association des consommateurs du Canada?

Mme Woodhead: Non. Je suis sûre que vous savez qu'en mars, nous avons eu des consultations avec le ministère de la Justice. Étaient représentés divers membres de l'industrie de

[Text]

various organizations, not companies. They were asked to attend that and politely declined. They said they had no interest in computer crime.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I see. But what about you people? Have you asked to join and be involved with the Consumers' Association of Canada?

Mrs. Woodhead: We have spoken to them. We have had members of our group as speakers at meetings of theirs, but we do not have any kind of formal relationship.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Just generally, how do you go about recruiting people into your organization, whether it is CIPS, the Canadian Information Processing Society, or one of your SIGs, Special Interest Groups?

Mrs. Woodhead: Well, the SIGs come mainly from CIPS membership. We advertise. It is within the CIPS budget; it is funded by CIPS. The rooms we meet in are provided by CIPS, etc., so we encourage CIPS members first and foremost to come to these groups. Our primary purpose is education of other data processors. That is, CIPS' role in life is to educate data processors.

Their secondary role is to educate the public on what data processors are up to, and this is where we are slowly moving. We are trying to catch up. We do have a large membership in our group which . . . Our SIG got a little complicated as it grew, being one of the first ones it sort of went off on its own merry way, and we spawned several sub-groups, one of which is on legislation. It has a sub-group on uniform law evidence.

Most of the members of these various other sub-groups are not CIPS members; they are lawyers, they are accountants, they are other professionals, and this is the way in which we really hope to contact other people in other industries. We are now very close to the Canadian Bar Association, we are very close to the Canadian Records Management Association and various other groups like that. We have a very good relationship and contact and exchange of information with some of these groups.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Are you in any way close to any of the police forces in Canada?

Mrs. Woodhead: Yes, we have membership in Toronto, we have RCMP, OPP and Metro-Toronto Police within our SIG. In Calgary, I believe, the RCMP are members out there as well. In Montreal, the QPP belongs, so we do have most of the police forces that are represented in any of the cities where the SIGs exist.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Where does your funding actually come from? You have indicated that your members are volunteers.

Mrs. Woodhead: Dues. You pay dues to belong to CIPS.

[Translation]

l'informatique, divers organismes; il ne s'agissait pas de compagnies. L'Association des consommateurs du Canada avait été invitée, mais avait poliment refusé en indiquant qu'elle n'était pas intéressée à la criminalité informatique.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je vois. En ce qui vous concerne, vous avez demandé à vous joindre à l'Association des consommateurs du Canada et à participer à ses travaux?

Mme Woodhead: Nous avons eu des communications avec l'association. Les membres de notre groupe ont eu l'occasion de prendre la parole à des réunions de l'association. Nous n'avons cependant pas de liens officiels.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): De façon générale, comment vous y prenez-vous pour recruter des gens, soit à l'Association canadienne de l'informatique, l'ACI, soit dans vos groupes d'intérêt particulier, les GIP?

Mme Woodhead: Les GIP sont formés surtout de membres de l'ACI. Nous faisons de la publicité. Nous avons un budget. Les salles où nous nous réunissons sont fournies par l'ACI, et le reste. Nous encourageons d'abord les membres de l'ACI à faire partie de ces groupes. Notre objectif principal est d'éduquer les informaticiens. C'est notre raison d'être, si vous voulez.

Notre deuxième but est d'éduquer le public sur l'activité des informaticiens. Nous progressons lentement sur ce plan. Nous essayons de rattraper le terrain perdu. Nous avons beaucoup de gens à l'intérieur de notre groupe . . . Notre GIP est devenu assez complexe avec le temps. Il a été l'un des premiers à se former, de sorte qu'il est devenu une entité distincte. Il a donné lieu à plusieurs sous-groupes, dont l'un s'occupe de la législation. Il y a un sous-groupe qui étudie la preuve et l'uniformité dans la loi.

La plupart des membres de ces sous-groupes n'appartiennent pas à l'ACI. Ce sont des avocats, des comptables, d'autres professionnels. C'est ainsi que nous espérons rejoindre les gens des autres secteurs. Nous avons actuellement des liens très étroits avec l'Association du barreau canadien, la *Canadian Records Management Association*, et des organismes semblables. Nous avons d'excellents échanges avec eux.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez des liens avec les forces policières au pays?

Mme Woodhead: Dans notre GIP de Toronto, nous avons des membres de la GRC, de la PPO et de la police du Toronto métropolitain. À Calgary, sauf erreur, nous avons également des gens qui nous viennent de la GRC. À Montréal, il y a des gens de la SQ. Donc, la plupart des forces policières des villes où nous avons des GIP sont représentées.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'où tirez-vous vos revenus? Vous avez indiqué que vos membres étaient bénévoles.

Mme Woodhead: Des cotisations versées à l'ACI.

[Texte]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You pay dues?

Mrs. Woodhead: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Do you mind telling us how much your dues are?

Mrs. Woodhead: They are \$125 a year in Toronto, that includes 10 dinner meetings, including dinner.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): This is per individual?

Mrs. Woodhead: Yes. And it varies from city to city, depending on whether the dinners are included or not.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I see. Is there a reduction if you get a company group joining or something like that?

Mrs. Woodhead: They are working on that. They do have what they call corporate memberships but it only allows a number of people; I am not exactly sure how it works. What they are trying to do is what IBM did several years ago, they are trying to unbundle, so that you can belong to CIPS without paying for the dinner meetings. You can just get the publications. You do not have to go out to any of the meetings. You can just sit back and receive information, or you can be actively involved and go out every month and attend, not only the dinner meetings, but the workshops that are put on, the technical lectures, the various special interest groups. We are trying to unbundle that so you can belong to any piece you want to.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You indicated that you support a code of ethics and that all the members of the Canadian Information Processing Society would be asked to sign such a code of ethics—I suppose as part of being a member. Have you drafted a code of ethics as yet, or do you have anything in mind?

Mrs. Woodhead: Yes. We have actually two. One was drafted by a national committee with CIPS members from across Canada and it is a much more general code of ethics, just basically what is good data processing practice, what is expected of you in your job. Our legislation sub-group last year prepared a privacy code of ethics. This is fairly new, it has just been released. It has been issued to the members in Toronto for review and comment and everything else. It is by no means anywhere close to becoming an actual code of ethics that people will sign, but at least it is getting out there to the membership of CIPS for some comment as to how they feel about it.

It would be signed by individuals, not organizations. We have absolutely no mandate to start asking companies to sign a privacy code of ethics.

[Traduction]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vos membres versent des cotisations?

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous voulez bien nous dire de combien sont ces cotisations?

Mme Woodhead: Elles sont de \$125 par année à Toronto, ce qui comprend 10 dîners-rencontres, dîner inclus.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Par personne?

Mme Woodhead: Oui. Le taux varie selon la ville, et selon que le dîner est inclus ou non.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je vois. Y a-t-il une réduction pour les groupes venant d'une compagnie, ou quelque chose du genre?

Mme Woodhead: Il y a une catégorie de membres de compagnies, mais elle ne prévoit que tant de personnes. J'ignore exactement comment le système fonctionne. Ce qu'on essaie de faire, c'est la même chose qu'IBM, il y a quelques années. On essaie de faire en sorte que les gens puissent appartenir à l'ACI sans avoir à payer les dîners. A ce moment-là, il est possible d'obtenir les publications de l'ACI, par exemple, sans avoir à aller aux réunions. Les gens pourraient se contenter de simplement recevoir l'information, ou encore ils pourraient décider de participer activement aux réunions mensuelles. Il n'y a pas que les dîners. Il y a des ateliers, des conférences techniques, des groupes d'intérêt particulier. On essaie actuellement d'en venir à offrir un choix.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez indiqué que vous êtes d'accord avec un code de déontologie et que tous les membres de l'Association canadienne de l'informatique devraient avoir à souscrire à un tel code. Vous en avez préparé un déjà, vous avez déjà une ébauche?

Mme Woodhead: De fait, nous en avons deux. Il y en a un qui a été préparé par notre comité national, formé de représentants de tout le Canada. Il est plus général et porte surtout sur les bonnes habitudes en matière d'informatique. Ce sont des qualités qu'on s'attend de trouver chez les informaticiens, si vous voulez. Par ailleurs, notre sous-groupe sur la législation a rédigé, l'année dernière, un code de déontologie privé. Il vient tout juste d'être publié. Il a été communiqué aux membres de Toronto, pour que ceux-ci fassent part de leurs réactions. Il n'est pas encore sur le point de devenir obligatoire, mais au moins, il a été communiqué aux membres de l'ACI. Ceux-ci peuvent faire leurs commentaires.

Ce serait les personnes mêmes, et non pas les organismes, qui s'y engageraient. Nous ne sommes absolument pas habilités à commencer à demander aux compagnies à souscrire à un code de déontologie sur le caractère privé des données.

[Text]

• 1615

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Could this committee obtain a copy of your draft code of ethics?

Mrs. Woodhead: Absolutely. I am afraid I do not have one with me, but I could certainly provide one.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have indicated these electronic data processing security officers, the EDP security officers, as you call them, are supposed to be involved wherever data processing is concerned.

Mrs. Woodhead: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): This, I assume, would be whether there were two or three people involved or a dozen or more people involved. You would still feel there should be what would be known as this EDP security officer.

Mrs. Woodhead: Yes. In many cases, it would be one of many responsibilities. You might have a senior DP person. If you have a shop of, say, only 10 people, you might assign one of those people in addition to his other duties to take security as one of those responsibilities.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): If there were one data processing person, then that person would be the security officer.

Now, is there any special training you would recommend for these people, or is there any special training they get at the present time? Where would they take this training? If it is reasonably extensive, would they contact community colleges? Do they have such a course at the present time, or could you suggest that maybe there should be such a course?

Mrs. Woodhead: To our knowledge, one university in Canada offers a course on computing ethics in their data processing curriculum, and it is an optional fourth-year course. There are no courses we know of for which you can pay your \$100 to \$200 and take. There are courses given by IBM, by manufacturers of various protection devices, including software and hardware. There are many, many, many books on the subject and articles that anybody who is even remotely interested in the field should read.

I cannot really say there is any set program that should be taken, but there is a basic bibliography that pretty well everybody in our group has in his office and refers to constantly. Perhaps if we published that, we would have the vague beginnings of a course; but to our knowledge, no course exists as such.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Are you planning on publishing some pamphlets on the requirements for security in data processing?

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Le Comité pourrait-il avoir une copie de votre projet de code de déontologie?

Mme Woodhead: Certainement. Je n'en ai pas avec moi aujourd'hui, mais je pourrais certainement vous la faire parvenir.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez dit qu'il devrait y avoir des agents de sécurité des systèmes de traitement électronique des données partout où il y a un service de traitement de l'information.

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Cela veut dire dans les services qui comptent deux ou trois personnes, comme dans ceux qui en comptent une douzaine ou plus. D'après vous, chaque service devrait avoir un agent de sécurité.

M. Woodhead: Oui. Dans bien des cas, il ne s'agirait pas d'une fonction unique. Un informaticien supérieur, par exemple, pourrait remplir cette fonction. Si vous avez un service qui compte seulement dix personnes, l'une d'elles pourrait être chargée de la sécurité du service, en plus de ses autres fonctions.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans ce service, s'il y avait un informaticien, c'est lui qui remplirait la fonction d'agent de sécurité.

Recommanderiez-vous une formation spéciale pour les agents de sécurité ainsi nommés, ou existe-t-il une formation spéciale à l'heure actuelle? Où obtiendrait-on cette formation? S'il s'agissait d'un programme relativement complet, ferait-on appel aux collègues communautaires? Existe-t-il un cours comme celui-là à l'heure actuelle, ou pourriez-vous recommander qu'il soit dispensé?

Mme Woodhead: À notre connaissance, une université, au Canada, offre un cours en matière d'éthique informatique dans son programme de traitement des données, et c'est un cours optionnel de quatrième année. Nous ne connaissons aucun cours auquel vous pouvez vous inscrire pour \$100 ou \$200. La compagnie IBM et les fabricants de divers dispositifs de protection offrent des cours sur le logiciel et l'équipement comme tel. Il existe de nombreux ouvrages sur le sujet, ainsi que des articles que devrait lire quiconque s'intéresse de près ou de loin au domaine.

Je ne peux pas vraiment dire qu'il existe un programme fixe à suivre, mais il y a quand même un certain nombre d'ouvrages de base que presque tous les membres de notre groupe possèdent dans leurs bureaux et consultent constamment. Peut-être que si nous publiions cette bibliographie, nous aurions un commencement de cours, mais à notre connaissance, il n'existe pas de cours comme tel.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Envisagez-vous de publier des brochures sur les

[Texte]

Mrs. Woodhead: Yes, we are; actually, in several ways. Our program for our group in Toronto for the past year has been what we called practical solutions to some of the more basic problems that any EDP security officer is going to encounter, and we are planning to make that available to CIPS members purely for the cost of reproduction. It will be notes and the slides people used in their presentations over the past year. We are going to be publishing a bibliography of books and articles, etc., that are available in the public domain, which are on the topic and are important articles. They bring forward new ideas, new concepts, new methods, new techniques, this kind of thing. So we will be publishing these kinds of things and making them available through CIPS.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Fine. You mentioned among some of your comments that we can prevent much computer crime. I assume from your statement—and, now, I am not taking you out of context—that you were saying, in effect, if people who use data processing equipment—and we are really talking about that area, I assume—if they carry out basic, fundamental security requirements, there would be very, very little crime at all.

Mrs. Woodhead: In fact, we do believe that to be true. We put on a session last year, actually, where we analysed about 12 known Canadian cases of some kind of computer abuse, whether we call it crime or not. Some of them may or may not have been. In each of those cases, we looked at what the law would or would not do and we looked at how it could have been prevented technically. In each case, we found there was some method that could have been implemented or used or was even implemented but not being used that could have prevented that event from happening.

What it requires is a budget; it requires a commitment. It requires communication with everybody who has anything to do with a particular computer on what the security precautions are, emphasizing that they have to follow those security precautions. They are not to give away their passwords. They are not to enter the building in the middle of the night and leave the door propped open, etc.

• 1620

The Acting Chairman (Mr. Robinson Etobicoke—Lakeshore)): You indicated that senior management do not seem to be too concerned. Is this general throughout the country with people who are doing data processing? They feel that the senior managers, the people above them, are really not concerned.

Mrs. Woodhead: Yes; one of the members of our group, a security officer for one of the big banks at a big data centre in Toronto, decided she would start publishing a newsletter about what is going on and what events have happened—court cases that are setting precedents and this kind of thing. She found that when this newsletter made it onto the vice president's

[Traduction]

besoins de sécurité dans le domaine du traitement de l'information?

Mme Woodhead: Oui; en fait, nous avons plusieurs projets. Le programme de l'année dernière, destiné à notre groupe de Toronto, portait sur des solutions pratiques aux problèmes les plus courants des agents de sécurité dans l'exercice de leurs fonctions, et nous avons l'intention de distribuer ce programme aux membres de l'ACI, en leur demandant seulement de payer le coût de reproduction. Il s'agira de recueils de notes et de diapositives qui ont servi aux exposés faits l'année dernière. Nous publierons une bibliographie de livres et d'articles importants sur le sujet qu'il est possible d'obtenir dans les librairies. Ces livres et articles traitent de nouvelles idées, de nouveaux concepts, de nouvelles méthodes et techniques, et ainsi de suite. Alors, ces choses-là seront publiées et mises à la disposition des intéressés par le biais de l'ACI.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Vous avez dit, entre autres, qu'il était possible de prévenir beaucoup de crimes informatiques. Est-ce à dire—et je ne vous cite pas hors contexte—que si les utilisateurs de matériel de traitement des données, et c'est vraiment d'eux qu'il est question, je suppose, prennent certaines précautions fondamentales, il y aura très peu de crimes?

Mme Woodhead: C'est ce que nous croyons effectivement. Nous avons organisé une réunion, l'an dernier, où nous avons analysé environ 12 cas d'infractions reliées aux ordinateurs au Canada, et qu'il se soit agi de crimes ou non n'a aucune espèce d'importance. Certaines infractions l'étaient peut-être, d'autres non. Dans chacun de ces cas, nous avons examiné ce que la loi pouvait ou ne pouvait pas faire, et nous avons déterminé comment l'infraction aurait pu être prévenue techniquement. Dans chaque cas, nous avons constaté que l'incident aurait pu être évité si quelques précautions avaient été prises.

Ce qu'il faut, c'est un budget; un engagement. Il faut sensibiliser aux mesures de sécurité à prendre tous ceux qui, de près ou de loin, ont quelque chose à voir avec l'ordinateur, et insister sur l'importance de suivre ces dispositions. Ils ne doivent pas divulguer leur mot de passe. Ils ne doivent pas pénétrer dans l'édifice au milieu de la nuit et laisser la porte entrouverte, etc.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez dit que les cadres supérieurs ne semblaient pas trop soucieux de la sécurité. Est-ce une idée bien répandue au pays chez ceux qui travaillent dans l'informatique? Estime-t-on que les cadres supérieurs ne sont vraiment pas intéressés?

Mme Woodhead: Oui. Un de nos membres, un agent de sécurité d'un gros centre de données d'une grande banque de Toronto a décidé de publier un bulletin sur les incidents et événements qui s'étaient produits—les affaires devant les tribunaux qui créent des précédents, et ainsi de suite. Quand son bulletin de nouvelles est parvenu au vice-président, celui-ci s'est empressé de descendre et lui a demandé: «Qu'est-ce que

[Text]

desk, he came racing downstairs and said: "What do you mean I cannot charge him for theft?". This is very typical.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): But until such time as there is a theft, or a trespass, or whatever you want to call it, there does not seem to be too much concern.

Mrs. Woodhead: That is right.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I understand that the focus of your organization is to get everybody involved in being more concerned about the security aspects of data processing.

Mrs. Woodhead: Yes; and as we do so, we have fingers pointed at us and we are called scare-mongering paranoiacs.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): There is a statement on page 2 of your notes, in the middle of the second paragraph, where you say: "He must examine every program and data file for criticality . . ."—I wonder what you meant by that—" . . . timeliness and the need for privacy . . .". You added the word "vulnerability" as well. Would you care to comment on this?

Mrs. Woodhead: Okay. One of the most common ways that people—particularly people who use IBM equipment—can protect their systems is by what we call a software access control package. This package goes on your computer and when you try to sign on to the computer, it asks you who you are, makes sure you are who you say you are and analyses which files it has got in there that you are allowed to use for your job, which ones you can look at but not do anything to, which ones you can write notes to but not print out . . . this kind of thing. It is an access table, basically.

To be able to implement any of this kind of access control you have to look at each program and file on the computer to see who should be able to use what for what purpose. This means: what is this program being used for? Who uses it? Is it a program that is being used by the payroll department so that a payroll clerk should be able to look at it but not write it out? Is it a program that is being used only by the systems developers and therefore no one else should be able to look at it? In terms of criticality, what I mean is: if your computer is lost to you today what programs would you absolutely need to have it back up and running by tomorrow morning, so your company can stay in business? This would probably mean your accounts receivable; it would probably mean your inventory . . . this kind of thing.

So you have to analyse each thing that is on the computer to see how relevant it is to your business; how long you could do without it; how vulnerable it is to misuse; how fast you would need it if it were not available; could you do without it for a month? Could you do without it for a week? This is the sort of thing he must be looking at constantly.

[Translation]

vous voulez dire, je ne peux pas le poursuivre pour vol?» C'est une situation très typique.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais tant qu'il n'y a pas de vol, ou de violation, ou appelez cela comme vous voudrez, on ne semble pas trop se soucier.

Mme Woodhead: C'est bien ça.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Votre organisme a comme objectif, je pense, de sensibiliser tous ceux qui travaillent dans le domaine de l'informatique à l'aspect sécurité de la chose.

Mme Woodhead: Oui, et on nous traite de paranoïaques alarmistes.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): A la page 2 de votre mémoire, au milieu du deuxième paragraphe, vous dites: «Il doit examiner chaque programme et chaque ensemble de données pour en déterminer l'importance . . .»—qu'entendez-vous par cela—« . . . l'opportunité et le caractère privé . . .». Vous avez ajouté le mot «vulnérabilité» aussi. Pourriez-vous m'expliquer un peu cela?

Mme Woodhead: Très bien. L'un des moyens les plus courants qu'on utilise, particulièrement avec l'équipement IBM, pour protéger les systèmes, c'est ce que nous appelons un programme de contrôle de l'accès au logiciel. Ce programme s'intègre à votre ordinateur, et quand vous vous apprêtez à utiliser l'ordinateur, celui-ci vous demande qui vous êtes, s'assure que vous êtes bien qui vous dites et analyse les ensembles de données que vous êtes autorisé à utiliser pour faire votre travail, détermine les données que vous pouvez consulter, mais pas modifier, les données auxquelles vous pouvez ajouter des notes, mais ne pas sortir sur imprimantes, et ainsi de suite. C'est essentiellement un tableau d'accès.

Pour pouvoir exercer un tel contrôle d'accès, vous devez examiner chaque programme et chaque ensemble de données intégrés à l'ordinateur, pour déterminer qui peut utiliser telle ou telle chose, et à quelle fin. Cela veut dire: à quoi sert ce programme? Qui l'utilise? S'agit-il d'un programme utilisé par le service de la paie qu'un commis à la paie devrait pouvoir consulter, mais pas reproduire? S'agit-il d'un programme utilisé seulement par ceux qui établissent des systèmes et auquel personne d'autre ne devrait avoir accès? Quand on parle d'importance, on veut dire: si votre ordinateur tombe en panne aujourd'hui, quel programme vous faudrait-il absolument pour le remettre en marche avant demain matin, pour que votre compagnie puisse demeurer en affaires? Cela veut probablement dire les comptes à recevoir, votre inventaire, et autres choses du genre.

Alors, vous devez analyser chaque élément d'information de votre ordinateur pour déterminer dans quelle mesure il est indispensable à votre entreprise; pendant combien de temps vous pouvez vous en passer; dans quelle mesure il est susceptible d'être utilisé abusivement; dans combien de temps vous en auriez besoin si vous en étiez privé; pourriez-vous passer un mois sans l'avoir? Pourriez-vous passer une semaine? Voilà ce dont il faut tenir compte constamment.

[Texte]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I see. You indicated in your statement that you are really not too concerned about the reporting of computer crime. I suppose the corporation, if that is the case, should have the option of just taking action against the employee through firing them, and not giving them a recommendation for another job in the same field and nothing further. Would you not feel that this reporting could be very important in the whole realm of deterrents?

Mrs. Woodhead: I personally do. What I have here is a group of people who would like to be able to say to the guy who is working for them: Look, we know you did a really bad thing; I could take you to court for this, but I think you deserve a second chance. This is the personal aspect these people are looking at.

They are also looking at the embarrassment of the company. We know that an awful lot of computer abuses are taking place and are not being reported because companies do not want to be publicly embarrassed; they do not want their stock holders, for instance, to know that they have just somehow lost \$2.5 million in some error, so they keep these things secret. This being the case, making that a crime would not serve anybody's purpose.

• 1625

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You mentioned the software access control package that is provided by computer outfits like IBM and so on, and I suppose by quite a number of those who produce computers. Is there, to your knowledge, any fail-safe mechanism in this package?

Mrs. Woodhead: No.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Just a straight no.

Has it ever been considered that there should be a back-up?

Mrs. Woodhead: Yes, but other than turning your computer off every night and, in the case of microcomputers, putting it in your back pocket and taking it home, there is no way you can really keep a computer 100% safe from everybody. What you have to do is somehow trade off what it is going to cost you to keep it safe from what it is going to cost you to lose it, and there has to be some fair shake there. To date, there is no cost-effective way of 100% protecting a computer.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): On page 3 of your notes, in the last paragraph, midway down, you make the statement:

Other data processors, systems designers, programmers, etc., do not understand the controls that must be implemented or what might be critical to the company's business.

What kind of controls are you really talking about that should be implemented and are probably not?

[Traduction]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je vois. Vous avez dit, dans votre déclaration, que vous n'étiez pas trop inquiète de la divulgation du crime informatique. Je suppose que la compagnie devrait simplement avoir le droit de renvoyer l'employé, sans lui donner une appréciation favorable pour qu'il obtienne un autre emploi dans le même domaine, et rien de plus. Ne pensez-vous pas que la divulgation du crime pourrait constituer un élément très important de dissuasion?

Mme Woodhead: Personnellement, je crois que oui. Mais j'ai un groupe de personnes, ici, qui aimeraient pouvoir dire à l'employé: eh bien, nous savons que vous avez fait quelque chose de très mal; je pourrais tenter des poursuites, mais je pense que vous méritez une chance. Voilà l'aspect personnel qui compte pour ces gens-là.

On tient compte également de l'embarras que cela peut causer à la compagnie. Nous savons qu'il y a énormément d'infractions relatives aux ordinateurs qui sont perpétrées et qui ne sont pas signalées parce que les compagnies ne veulent pas d'embarras; elles ne veulent pas que leurs actionnaires, par exemple, sachent qu'elles ont perdu 2.5 millions de dollars à cause d'une erreur quelconque; alors, elles n'en parlent pas. Alors, cela n'aiderait personne que ce soit un crime de ne pas signaler une infraction.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé de programmes de contrôle d'accès au logiciel que produisent certaines compagnies, comme IBM, et bien d'autres fabricants d'ordinateurs, je suppose. A votre connaissance, existe-t-il un mécanisme à toute épreuve?

Mme Woodhead: Non.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Un non catégorique.

A-t-on déjà pensé qu'il faudrait un système d'appoint?

Mme Woodhead: Oui, mais outre le fait de fermer votre ordinateur chaque soir et, dans le cas de micro-ordinateurs, de le glisser dans votre poche et de l'apporter à la maison, il n'y a vraiment aucun moyen à toute épreuve d'empêcher que quelqu'un se serve de votre ordinateur. Vous devez faire une étude de rentabilité et peser le coût des dispositifs de sécurité par rapport au coût de la perte de votre système, et ensuite, choisir ce qu'il convient de faire. A l'heure actuelle, il n'y a aucun dispositif de sécurité à toute épreuve qui soit rentable.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À la page 3 de votre déclaration, au milieu du dernier paragraphe, vous dites:

D'autres informaticiens, concepteurs de systèmes, programmeurs, et ainsi de suite, ne comprennent pas les dispositifs de contrôle qu'il faut mettre en place, ou ce qui est essentiel pour la compagnie.

Quel genre de dispositifs de contrôle devrait-il y avoir, d'après vous?

[Text]

Mrs. Woodhead: Okay. Systems programmers are the key to any data processing department. They are the people who keep the computer running, make it work better, add things to it, enhance it, etc. For these people to be able to do their jobs, they claim they must have access to everything on the system. This is, in fact, to a certain extent true, but systems programmers are also noted for prima donna type attitudes. When you try to implement a software access control package, for instance, and restrict your systems programmers to only a particular part of the system at any one time, they will say they are unable to do their jobs.

They do not respect the fact that they are a risk as well as the guy playing with the payroll system. They feel they must have all freedoms at all times. So they do not understand why controls should be placed in their way, and, to a very large extent, particularly in the very large organizations such as banks, your data processing department does not really understand the business that the company is in. They understand how to write programs to make something do what you want it to do, but they do not understand banking. So they do not understand what kinds of risks, for instance, this particular trust company might face because of the particular business it is in, as opposed to that manufacturing company over there.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have a list of points that explain your point of view with regard to what would be considered as new legislation that should be required in this field of computer abuse. I am wondering, do you consider there should be any changes to the Criminal Code, or are you really feeling it should be a new statute, or should we just have amendments to, say, the Copyright Act, the Patent Act, and some others?

Mrs. Woodhead: I think the group is fairly well in agreement that there should be amendments to the Copyright Act or to the Trade Secrets Act. That would only deal with part of the problem; that would deal with protection of software packages, etc.—you will be able to copyright your software and therefore people cannot walk off with it. But I think what they would really like to see is an amendment, such as was done for theft of credit cards under the Theft Act in the Criminal Code, where stealing something from a computer is a criminal act.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So you are really suggesting there should be both.

Mrs. Woodhead: Yes. From what I have heard about the copyright amendments, etc., etc., they are under way. I am not quite sure what stage they are at.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Now, when you were talking about the reporting of computer crime, you had it within the context of what I might call the internal situation, within the company itself, but what about the external? Do you figure it should not be reported there either, not necessarily?

[Translation]

Mme Woodhead: Bien. Les programmeurs sont la clé de tout service de traitement des données. Ce sont eux qui assurent le fonctionnement de l'ordinateur, qui améliorent son rendement, qui y ajoutent des choses, et ainsi de suite. Ces gens-là prétendent que, pour faire leur travail, ils doivent avoir accès à tous les éléments du système. Jusqu'à un certain point, c'est vrai, mais les programmeurs sont aussi réputés pour leur attitude de prima donna. Si vous essayez d'établir un programme de contrôle d'accès au logiciel, par exemple, et si vous limitez l'accès des programmeurs à une partie seulement du système, ils vous diront qu'ils ne peuvent pas faire leur travail.

Ils ne respectent pas le fait qu'ils constituent eux-mêmes un risque, au même titre que celui qui utilise le système de paye. Ils pensent qu'ils doivent toujours être entièrement libres. Ils ne comprennent pas pourquoi ils devraient s'embarrasser de dispositifs de contrôle et, de façon générale—particulièrement dans les très grosses institutions, comme les banques—le service de traitement des données ne comprend pas vraiment ce que fait la compagnie. Les employés du service savent comment établir des programmes pour répondre à vos besoins, mais ils ne savent pas ce que c'est qu'une banque. Alors, ils ne comprennent pas la différence entre les risques avec lesquels doit composer, par exemple, une compagnie de fiducie, à cause de la nature même de ses affaires, et les risques d'une compagnie manufacturière.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez présenté une liste de cinq recommandations faisant état de ce que devrait comporter une nouvelle loi sur les crimes informatiques. Pensez-vous qu'il faudrait apporter des modifications au Code criminel, ou pensez-vous qu'il faudrait une loi complètement nouvelle, ou devrions-nous simplement modifier la Loi sur le droit d'auteur ou la Loi sur les brevets, et certaines autres?

Mme Woodhead: Je pense que le groupe convient généralement qu'il faudrait apporter des modifications à la Loi sur le droit d'auteur ou à la Loi sur les secrets industriels. Mais cela ne résoudrait qu'une partie du problème: les logiciels pourraient ainsi faire l'objet d'un droit d'auteur, et personne ne pourrait les prendre. Mais ce qu'on aimerait vraiment, c'est un amendement comme celui qui a été apporté pour les cartes de crédit, aux termes des dispositions du Code criminel concernant le vol, de sorte qu'il soit établi que le vol d'un élément d'information d'un ordinateur constitue un acte criminel.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il faudrait donc faire les deux.

Mme Woodhead: Oui. D'après ce que j'ai entendu dire au sujet des amendements concernant le droit d'auteur, il semblerait que les travaux avancent. Je ne suis pas sûre à quel point on en est rendu.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Quand vous avez parlé de la divulgation du crime informatique, vous parliez surtout d'infractions perpétrées de l'intérieur de la compagnie, mais qu'en est-il des infractions perpétrées de l'extérieur? Pensez-vous qu'elles ne devraient pas être signalées elles non plus?

[Texte]

• 1630

Ms Woodhead: Do you mean an external perpetrator?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes.

Ms Woodhead: I would think it would have to be. There is no way you can discipline an external person.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): Okay. In your case, with regard to this paper, you are referring particularly to people who are involved in data processing...

Ms Woodhead: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): —people such as yourself. Are you a data processor?

Mrs. Woodhead: I am a consultant.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): But you have done data processing?

Mrs. Woodhead: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): You are just above that now, advising others, I suppose.

Mrs. Woodhead: That is right.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): But you know what data processing is all about. I get the general impression, or a kind of theme throughout your paper, that what you are saying is: We can sort of self-regulate, we can sort of self-control; we are building up this organization to try to control the operation and we want to be able, in effect, to discipline ourselves. Would that be a fair statement to make?

Mrs. Woodhead: Yes, I think that would be a fair statement.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): Therefore, you would rather it be left up to the people in the business to decide whether in fact reporting is or is not necessary?

Mrs. Woodhead: Yes. If it becomes a crime not to report, we are going to have an awful lot of criminals out there.

The Acting Chairman (Mr. Robinson (Etobicoke... Lakeshore)): You spoke of formulas for evaluating what data to protect. How do these formulas work?

Mrs. Woodhead: This is commonly called risk analysis. The basic theory is that your exposure, which would be your loss from any one event, times the probability of that event, equals your annual expected loss. That sounds very pat, but it is a very difficult thing to do. If, for instance, your whole data processing department were unavailable to you for a month, trying to evaluate that as to what your exposure is, what the dollar value is of that unavailability, requires an awful lot of digging and interpreting in trying to reconstruct data—how much does it cost to reconstruct this file as opposed to that file,

[Traduction]

Mme Woodhead: Vous voulez dire quelqu'un de l'extérieur?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui.

Mme Woodhead: Cela ne pourrait être autrement. Il est impossible de discipliner quelqu'un de l'extérieur.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): D'accord. Dans votre document, vous parlez tout particulièrement de personnes s'occupant de traitement de données...

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): ... de personnes comme vous-même. Êtes-vous informaticienne?

Mme Woodhead: Je suis expert-conseil.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais vous avez fait du traitement de données?

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez maintenant dépassé ce stade et vous conseillez les autres, je suppose.

Mme Woodhead: C'est exact.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mais l'informatique est quelque chose que vous connaissez très bien. J'ai l'impression qu'un leitmotiv revient tout au long de votre document, vous répétez tout le temps: Nous pouvons nous autocontrôler, nous pouvons nous autoréglementer; nous mettons sur pied cette organisation pour essayer de contrôler les opérations et nous voulons, en fait, être en mesure de nous discipliner nous-mêmes. Est-ce que je traduis bien votre pensée?

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Par conséquent, vous préféreriez qu'on vous laisse le soin de décider s'il est nécessaire ou non de rapporter les délits.

Mme Woodhead: Oui. Si ne pas rapporter les délits devient en soi un délit, le nombre de délinquants sera impressionnant.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé de formules pour évaluer quelles données protéger. Comment fonctionnent ces formules?

Mme Woodhead: C'est ce qu'on appelle communément le calcul des risques. Il s'agit simplement de multiplier le risque de perte par la probabilité de son éventualité, ce qui vous donne la perte éventuelle par année. Cela semble très simple, mais c'est très difficile à réaliser. Si, par exemple, tout votre service d'informatique ne fonctionne pas pendant un mois, essayer d'évaluer cette absence de risque, la valeur en dollars de cette absence de risque, nécessite beaucoup de calculs et d'interprétations, de reconstitution de ces données, combien cela peut-il coûter pour reconstituer ce dossier plutôt que cet

[Text]

can we replace this computer part in a week, or does it take a month. That is the kind of analysis that has to go into effect there. When you look at probability, statistics in Canada are very hard to get and are usually 20 years out of date. But when you look at something like the Mississauga rail disaster, which happened four years ago now . . .

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): You are talking about the risk analysis with regard to data, the software in effect, not the hardware?

Mrs. Woodhead: Anything—your computer department.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): I see. Is one of the aspects you look at the cost, as well—the risk, the cost, and the cost is part of your analysis?

Mrs. Woodhead: Yes.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): How serious are the abuses you have seen in your time of being involved with this organization and in being involved with data processing and how widespread are the abuses?

Mrs. Woodhead: They are probably not as widespread as some people would like us to believe. We are always reading in the press that we are only seeing the tip of the iceberg and there is probably 500 times what we read about actually going on and that each particular event is costing 10 times the amount that white-collar crime used to cost. We do not feel it is probably as bad as all that, but I would say that there is not a computer shop in Canada that does not have some kind of abuse. How serious that abuse is and whether it should be addressed by the Criminal Code, or whether the fellow should be fired, or whether the security officer should just tighten up his act a little, is very debatable. But I cannot think of a single computer operation that has not abused its computer in some way or other.

The Acting Chairman (Mr. Robinson (Etobicoke — Lakeshore)): You indicated that minimum efforts should be taken to protect the software—and the hardware too, for that matter. Do you have any suggestions to make as to how this can be done?

Mrs. Woodhead: Not at the present time. There is the example that was taken by the Foreign Corrupt Practices act, just that if you, for instance, expose somebody's private information and he sues and gets \$2 million, that particular individual who allowed that event to happen, through not exercising tighter control, is personally liable for that \$2 million. I think that is probably a bit heavy for Canadians and probably not a realistic way of going about it. But something along the lines that a particular individual or a particular group of individuals within an organization somehow have to be pointed at and said you have to place a certain emphasis on this subject; you cannot just pay lip-service to it and you cannot ignore it; it has to be addressed.

[Translation]

autre, peut-on remplacer cet élément d'ordinateur en une semaine ou faut-il un mois. C'est le genre d'analyse qu'il faut faire. Quand on veut faire des calculs des probabilités, au Canada il est très difficile d'obtenir des statistiques et généralement elles ont 20 ans de retard. Si vous prenez l'exemple de la catastrophe ferroviaire de Mississauga qui a eu lieu il y a maintenant 4 ans . . .

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous parlez du calcul de risques concernant les données, concernant en fait le logiciel et non pas le matériel?

Mme Woodhead: Tout ce qui constitue les services d'informatique.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je vois. Lorsque vous faites ces calculs de risques, y incluez-vous également le coût?

Mme Woodhead: Oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Quelle est l'ampleur des abus et des délits que vous avez constatés depuis que vous travaillez pour cette organisation et depuis que vous travaillez dans le monde de l'informatique?

Mme Woodhead: Ce n'est probablement pas aussi important que certains voudraient nous le faire croire. La presse ne cesse de répéter que ce n'est que la pointe de l'iceberg et qu'il faut probablement multiplier par 500 fois pour arriver à un chiffre exact et que chaque événement particulier coûte 10 fois plus cher que les crimes en col-blanc ne coûtaient. Nous ne pensons pas que le tableau soit aussi sombre, mais j'ajouterais qu'il n'y a pas un seul service d'informatique au Canada qui n'ait subi une forme ou une autre de délit. Déterminer la gravité de ces délits, les faire tomber sous le coup du Code criminel, congédier les responsables ou sensibiliser et sermonner les agents de sécurité est controversable. Je ne pense pas cependant connaître un seul service d'informatique qui n'ait pas subi ce genre d'abus.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez dit que des efforts minimums devraient être faits pour protéger le logiciel, et le matériel d'ailleurs. Avez-vous des suggestions?

Mme Woodhead: Pas pour le moment. Il y a l'exemple de la Foreign Corrupt Practices Act qui a déjà été invoqué. Si les renseignements privés d'une personne sont divulgués, qu'elle vous poursuive et qu'elle obtienne 2 millions de dollars, celui qui est à l'origine de cette divulgation par négligence est tenu personnellement responsable et doit payer ces 2 millions de dollars. Ce serait un peu lourd pour les Canadiens et une méthode peu réaliste de régler le problème. Il serait préférable de faire comprendre au responsable ou aux responsables de ces services l'importance de ce problème qui ne peut ni être traité à la légère ni être ignoré.

[Texte]

• 1635

In fact, this is happening to a certain extent, as I mentioned earlier, with these access control packages, particularly on IBM computers. I know of very few that do not have some kind of access control package in place. It is basically becoming an industry standard. It may be that through the courts somehow we will establish what other companies have accepted as a minimum standard, and if this particular company who has been victimized is not up to that level he himself or his company is somehow responsible, not the person who perpetrated the crime. I am not sure how that might work, but the industry is establishing some standards. It is very unusual, for instance, to have a large-scale IBM computer without an access control package.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): On the last page of your notes in the first paragraph at the last sentence you say:

In the final analysis, the perpetrator should be punishable for antisocial behaviour.

Could you explain what you mean by that? It would seem to me that when you talk about antisocial behaviour you are talking about people who are sick or who have an illness. Or do you feel that this is really criminal behaviour for which they should be punished?

Mrs. Woodhead: What I mean is that I feel that through its laws society says what is acceptable and ethical. It says theft is illegal; it is not acceptable behaviour. I believe that if computer abuse were a crime then society would be saying in effect this is not acceptable behaviour. Therefore by perpetrating some kind of computer abuse you are in effect behaving antisocially: you are going against what society has said is and is not ethical, moral, acceptable behaviour.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose it is fair to say at present, since there is no such thing as a computer crime per se, that...

Mrs. Woodhead: That is antisocial.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): —all we can say is that it is a bit of antisocial behaviour. Is that it? So until we have a statute that makes it an offence, or an amendment to the Criminal Code that makes it a crime, we are just talking about antisocial behaviour.

Mrs. Woodhead: Actually, what I meant was if and when it becomes a crime it is therefore antisocial because it is against what society has deemed to be allowable.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You spoke of specific offences. What would these specific offences be? Would it be abuse of the computers, a trespass? What kind of offences are you really talking about?

Mrs. Woodhead: I think probably trespass, taking the common connotation of trespass as being somewhere you are

[Traduction]

C'est ce qui se fait d'ailleurs dans une certaine mesure, comme je l'ai déjà mentionné, avec ces systèmes de contrôle d'accès accompagnant tout particulièrement les ordinateurs de chez IBM. J'en connais très peu qui ne comportent pas ce genre de systèmes. Cela devient de plus en plus la norme dans l'industrie. Il est possible que par l'intermédiaire des tribunaux, nous finirons par établir ce que les autres compagnies acceptent comme norme minimum, et si la compagnie victime d'un délit n'applique pas elle-même cette norme minimum, c'est elle en quelque sorte qui est responsable et non pas la personne ayant perpétré le délit. Je ne sais encore comment cela pourrait fonctionner, mais l'industrie établit certaines normes. Il est très inhabituel, par exemple, d'avoir un gros modèle d'ordinateur de chez IBM sans système de contrôle d'accès.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): A la dernière page de vos notes, vous dites dans la dernière phrase du premier paragraphe:

En dernière analyse, l'auteur du délit devrait être puni pour conduite antisociale.

Pourriez-vous m'expliquer ce que vous entendez par là? Je penserais plutôt qu'on parle de conduite antisociale pour des gens malades. Ne considérez-vous pas cela comme une conduite criminelle qui devrait être punie?

Mme Woodhead: J'estime que par ces lois, la société indique ce qu'elle considère comme acceptable et moral. Elle dit que le vol est illégal, que ce n'est pas une conduite acceptable. Je crois que si la truandique était considérée comme un délit, la société jugerait en effet que ce n'est pas une conduite acceptable. Par conséquent, en vous livrant à une certaine forme de truandique, vous vous conduisez d'une manière antisociale: vous allez à l'encontre de ce que la société considère comme moral, comme conduite acceptable.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je suppose qu'étant donné qu'à l'heure actuelle, ces délits liés à l'informatique n'existent pas en tant que tels, que...

Mme Woodhead: C'est antisocial.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): ... tout ce que nous pouvons dire, c'est que c'est une conduite un peu antisociale. N'est-ce pas? Tant que nous n'aurons pas une loi en faisant un délit, ou un amendement au Code criminel en faisant un crime, nous ne pourrions que parler de conduite antisociale.

Mme Woodhead: En réalité, je voulais dire que lorsqu'on considérera cela comme un crime, cela sera par conséquent antisocial puisque contraire à ce que la société juge acceptable.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous avez parlé de délits précis. Quels sont-ils? L'utilisation non autorisée? De quel genre de délits voulez-vous vraiment parler?

Mme Woodhead: D'utilisation non autorisée, d'utilisation de l'ordinateur à une fin non prévue, d'utilisation de l'ordinateur

[Text]

not supposed to be, is probably the most common offence: people using the computer for something it was not intended for, being on the computer for something other than their own job. The best example is playing *Star Wars* on Friday afternoons. This is trespassing on your company's computer.

The second probably most common occurrence would be some kind of equivalent to break and enter, where you get access to a computer system and files and data that have been barred from you by not giving you the telephone number, by not giving you the password, this kind of thing. They have tried to put a barrier in between and you have somehow gotten around that barrier and you have broken and entered in some way. Along with that would go once you are inside the computer manipulating the information either for personal gain or for the hell of it; both are probably equally common. The horror stories are of the people who somehow got into a computer where they were not supposed to be and started playing around with information and have ended up with bank accounts that were not supposed to exist or companies being paid that never delivered goods and this kind of thing.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): The last question I want to ask you has to do with standard of care. Are you making any headway with the standard of care, particularly with regard to the people who are data processors? Are you making any headway with the corporations, say, who have the machines and with their personnel? How much headway, if any, are you making?

• 1640

Mrs. Woodhead: We are making headway among data processors as a group. We are making headway with other professions such as accountants. They now understand far better than they did three years ago what some of the problems are, what they should be looking for, how they should be looking for it. We are making headway with lawyers. They now have a much better understanding of what is required, for instance, in a computer contract so that we do not let these things slide through as they have done in the past. We are not making a lot of headway with the public at large. I am not really sure how one goes about that. But we are definitely making headway with universities, as well, with the academic world, trying to show them that we do need the universities to take some responsibility for turning out people with some concept of what is right and wrong in this environment.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you, Mrs. Woodhead, for your excellent presentation, giving us another view that we had not heard before.

I thank you very much for coming and appearing before the committee. If you are preparing any material, including a so-called code of ethics, if you would send it along we would be only too glad to have it.

Mrs. Woodhead: Absolutely.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Whether we receive it before we write our report or afterwards, we would still like to receive it, because we will

[Translation]

à une fin n'ayant rien à voir avec le travail de l'utilisateur. Le meilleur exemple est de jouer à la guerre des étoiles le vendredi après-midi. C'est une utilisation non autorisée de l'ordinateur de la compagnie.

Ensuite, ce qui est probablement le plus courant et qui pourrait être comparé à l'effraction pure et simple, c'est-à-dire accéder à un réseau informatisé et à des données protégé par un numéro de téléphone, par un mot de passe auquel vous n'avez pas droit. Une barrière a été dressée entre vous et ces informations, barrière que vous êtes parvenu à contourner et votre accès s'est fait par effraction. De plus, une fois cet accès réalisé, il peut y avoir manipulation des données à des fins de gains personnels ou simplement pour s'amuser; ces deux fins sont probablement aussi communes. On entend parler de gens qui, après avoir accédé par effraction à des réseaux informatisés, se sont constitué des comptes bancaires inexistantes ou des compagnies se faisant payer pour des marchandises jamais livrées, etc.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Ma dernière question portera sur les normes de sécurité. Faites-vous des progrès, surtout au niveau des informaticiens? Faites-vous des progrès avec les sociétés possédant ces machines et avec leur personnel? Quels progrès, s'il y a progrès, faites-vous?

Mme Woodhead: Nous faisons des progrès chez des informaticiens en tant que groupe. Nous faisons des progrès chez les autres professionnels comme les comptables. Ils comprennent maintenant beaucoup mieux qu'ils ne le comprennent il y a trois ans certains des problèmes, que chercher et comment chercher. Nous faisons des progrès avec les avocats. Ils comprennent mieux maintenant ce qui est nécessaire, par exemple, dans un contrat d'ordinateur et comblent ces lacunes qui existaient auparavant. Nous ne faisons pas beaucoup de progrès auprès du grand public. Par contre, nous faisons définitivement des progrès dans le monde universitaire en démontrant aux enseignants la nécessité d'inculquer des principes de bien et de mal dans cet environnement.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Madame Woodhead, je vous remercie de votre excellent témoignage qui nous a exposé un point de vue que nous n'avions pas encore entendu.

Je vous remercie infiniment d'être venue et d'avoir comparu devant notre Comité. Si vous préparez des documents, y compris ce code de déontologie, nous aimerions infiniment les recevoir.

Mme Woodhead: Absolument.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Que nous les recevions avant de rédiger notre rapport ou après, nous aimerions quand même les recevoir, car

[Texte]

probably be keeping a file on this whole matter. So thank you once again for coming.

The subcommittee will resume consideration of its order of reference on Thursday, May 26, 1983, at 9.30 a.m. in this same room, Room 208, West Block, with representatives from The Canadian Bankers' Association.

The meeting is adjourned.

[Traduction]

nous garderons probablement un dossier à ce sujet. Une fois de plus, je vous remercie d'être venue.

Notre Sous-comité reprendra l'examen des questions figurant à son ordre de renvoi le jeudi 26 mai 1983 à 9h30, dans la même salle, la salle 208 de l'Édifice de l'ouest, et les témoins seront les représentants de l'Association des banquiers canadiens.

La séance est levée.











If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESS—TÉMOIN

From the Canadian Information Processing Society, Toronto:

Mrs. Sally Woodhead, Chairman, Special Interest Group on
Computer Security.

De la «Canadian Information Processing Society», Toronto:

M^{me} Sally Woodhead, présidente, Groupe spécial d'intérêt
sur la sécurité informatique.

HOUSE OF COMMONS

Issue No. 13

Thursday, May 26, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 13

Le jeudi 26 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

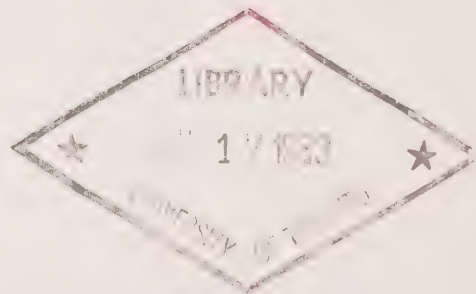
Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

THURSDAY, MAY 26, 1983
(15)

[Text]

The Sub-committee on computer crime met this day at 9:46 o'clock a.m., the Acting Chairman, Mr. Ken Robinson (*Etobicoke—Lakeshore*), presiding.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From the Canadian Bankers' Association: Mr. R.M. MacIntosh, President; Mr. E. Jestin, Supervisor—Internal Control, Evaluation, The Bank of Nova Scotia, and Ms. Pat Learmonth, Co-ordinator of Communications.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

Mr. MacIntosh and Ms. Learmonth made statements and, with Mr. Jestin, answered questions.

On motion of Mr. Beatty, it was ordered, that the brief entitled "Bill S-33, the Canada Evidence Act, 1982" submitted by the Canadian Bankers' Association to the Senate Standing Committee on Legal and Constitutional Affairs, on Tuesday, May 10, 1983, concerning Bill S-33, An Act to give effect, for Canada to the Uniform Evidence Act adopted by the Uniform Law Conference of Canada, be printed as an appendix to this day's Minutes of Proceedings and Evidence. (*See Appendix "COMP-2".*)

At 11:12 o'clock a.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE JEUDI 26 MAI 1983
(15)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 9h46, sous la présidence de M. Ken Robinson (*Etobicoke—Lakeshore*), président suppléant.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: De l'Association canadienne des banquiers: M. R.M. MacIntosh, Président; M. E. Jestin, Superviseur, Vérification et évaluation interne, La Banque de Nouvelle-Écosse et M^{lle} Pat Learmonth, co-ordinatrice des communications.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

M. MacIntosh et M^{lle} Learmonth font des déclarations et, avec M. Jestin, répondent aux questions.

Sur motion de M. Beatty, il est ordonné que le mémoire intitulé «Projet de loi S-33, Loi fédérale de 1982 sur la preuve» présenté par l'Association canadienne des banquiers au Comité sénatorial permanent des Affaires juridiques et constitutionnelles, le mardi 10 mai 1983, relativement au projet de loi S-33, Loi donnant effet pour le Canada à la Loi uniforme sur la preuve adoptée par la Conférence canadienne de l'uniformisation du droit, soit imprimé en appendice aux procès-verbaux et témoignages de ce jour. (*Voir appendice «COMP-2».*)

A 11h12, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

*(Recorded by Electronic Apparatus)**[Texte]*

Thursday, May 26, 1983

• 0947

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Ladies and gentlemen, we will come to order and start our meeting. Our order of reference is that the subcommittee resumes consideration of the order of reference, which is Mr. Beatty's bill on computer crime. We have before us a number of witnesses from the Canadian Bankers' Association: Mr. R. M. MacIntosh, President of the Canadian Bankers' Association—just indicate yourselves as we call out your names if you would—Mr. E. (Ted) Jestin, Supervisor, Internal Control Evaluation, The Bank of Nova Scotia; Mr. Michael Ballard, Director of Security, Canadian Bankers' Association; Ms Pat Learmonth, Co-ordinator of Communications, Canadian Bankers' Association, and Mr. Dan J. Sullivan, Public Affairs Adviser to the Canadian Bankers' Association.

I want to thank you for presenting us with your statement ahead of time. We have had a chance to read it, and we will have a few questions for you, but I would like you to consider going through the submission itself, which will be more than helpful, and I think Mr. Beatty and I will both have some questions for you.

So without further ado we will call upon the first witness, and then from there you can lead on to your colleagues if they have something to add to your statement.

Mr. R.M. MacIntosh (President, Canadian Bankers' Association): Thank you, Mr. Chairman. We appreciate the opportunity to appear before this subcommittee. I would like to make a few opening general remarks about computer crime before summarizing our brief.

In general, one thing we want to say to you is that the occurrence of computer crime is so rare an event in Canada that it is almost unknown. We have had a great deal of difficulty in identifying any cases at all in the banking industry which could be called computer crime. We have conducted a survey through our security division of the police forces in Canada to try to find out what cases they had identified of computer crime. Through a survey which we made fairly recently they were able to identify 33 possible cases which had occurred in Canada, although it is doubtful whether some of them could be classified as computer crime at all, and only one of those might have been attributed to being a computer crime case in a bank.

The first point I want to make is that the media stories which have appeared and the comments which have been made by so-called professionals about the subject have been very greatly exaggerated. Computer crime is more a question of myth than of fact.

TÉMOIGNAGES

*(Enregistrement électronique)**[Traduction]*

Le jeudi 26 mai 1983

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Mesdames et messieurs, je déclare la séance ouverte. Notre ordre de renvoi est que notre Sous-comité reprenne l'étude de son ordre de renvoi concernant le projet de loi de M. Beatty sur les infractions relatives aux ordinateurs. Nous recevons ce matin un certain nombre de représentants de l'Association des banquiers canadiens: M. R.M. MacIntosh, président de l'Association des banquiers canadiens—voudriez-vous vous identifier une fois que je citerai votre nom, s'il vous plaît—M. E. (Ted) Jestin, superviseur, Évaluation du contrôle interne, Banque de Nouvelle-Écosse, M. Michael Ballard, directeur de la Sécurité, Association des banquiers canadiens, M^{me} Pat Learmonth, coordonnatrice des services de communication, Association des banquiers canadiens et M. Dan. J. Sullivan, conseiller en affaires publiques de l'Association des banquiers canadiens.

Je tiens à vous remercier de nous avoir fait parvenir votre déclaration à l'avance. Nous avons eu la possibilité de la lire, et nous aurons quelques questions à vous poser. Cependant, j'aimerais que vous fassiez un petit résumé de votre mémoire, ce qui nous serait fort utile, et ensuite M. Beatty et moi-même vous poserons quelques questions.

Sans plus attendre, je donnerai donc la parole au premier témoin et ensuite vos collègues pourront ajouter quelque chose s'ils le désirent.

M. R.M. MacIntosh (président, Association des banquiers canadiens): Merci, monsieur le président. Nous vous remercions de nous avoir invités à comparaître. J'aimerais faire quelques remarques préliminaires au sujet des infractions relatives aux ordinateurs avant de résumer notre mémoire.

Nous tenons tout d'abord à vous dire que les infractions relatives aux ordinateurs sont si rares au Canada qu'elles sont pratiquement inconnues. Il nous est très difficile de désigner une seule affaire dans l'industrie bancaire pouvant être considérée comme une infraction relative aux ordinateurs. Nos services de sécurité ont mené une enquête auprès des forces de police canadiennes pour essayer de déterminer quelles affaires ces dernières avaient classées comme infractions relatives aux ordinateurs. Elles ont pu nous rapporter l'existence de 33 affaires possibles au Canada, bien qu'il soit tout à fait douteux que certaines d'entre elles puissent être classées comme infractions relatives aux ordinateurs, et seule une de ces affaires aurait pu être classée comme une infraction relative aux ordinateurs touchant une banque.

Je tiens tout d'abord à vous dire que les articles parus dans les médias et les commentaires faits par les soi-disant professionnels de cette question sont très grandement exagérés. Les infractions relatives aux ordinateurs sont plus un mythe qu'un fait.

[Texte]

• 0950

One of the problems is to define what computer crime is. And very frequently, if you look closely, you will see that what is said to be a computer crime is nothing more than a question of bad business practice. The committee may have heard about the series that was run in *The New Yorker* magazine about 10 years ago dealing with computer crime in the United States. Most of the cases that were dealt with in that series, at that time, had nothing to do with computer crime as such, they had to do with the fact that ordinary common sense, good business practice, was not followed in the cases at issue—for instance, where you do not have an audit and control system separate from your accounting system so that you can have an independent audit check.

It is ordinary good business practice in a bank to separate the programming and design of software systems from the operation of computer systems. That is an ordinary business practice. But more generally, in a bank or in any institution, for that matter, or any business, good control systems where you separate the accounting system from the audit of it is one of the factors which is not practised in so-called computer crime cases.

There have been some books written in Canada and some articles in which computer crime was identified as a serious problem. For instance, in Mrs. Granger's books about banking, she talks in somewhat scare language about computer crimes in Canada. In fact, all the cases which she cited were American cases. There were no Canadian cases whatsoever.

I will give you another recent example which happened to be published April 25, 1983, in *The Globe and Mail*. In this article Professor Anne Kittler of Ryerson Polytechnical Institute talked about the invasions of privacy caused by the computer, and I just want to cite a couple of examples of cases where the public can be greatly misled by the sort of thing which is being said and published.

In this article she says:

At a local financial institution, a programmer deposited into his own account the fractions of cents created by interest calculations, and amassed close to \$100,000 in a short time.

This paragraph is written in the context as though it were something that had occurred in Canada. Well, it never occurred in Canada, it occurred in the United States and 15 years ago. And this is being constantly referred to as the example, the prototype of computer crime where somebody takes off a small amount and large numbers in order to profit by it.

That is a chestnut case that occurred a long time ago. I do not know the exact circumstances of it, but it certainly was not in Canada in any event.

In the next paragraph she says:

Last summer it came to light that the Canadian Imperial Bank of Commerce had been bilked of about \$10 million

[Traduction]

Un des problèmes est de définir ce qu'on entend par infraction relative aux ordinateurs. Très souvent, en y regardant de plus près, on constate que ce que l'on taxe d'infraction relative aux ordinateurs n'est rien de plus qu'une question de mauvaise administration. Vous avez peut-être entendu parler de la série d'articles sur les infractions relatives aux ordinateurs aux États-Unis publiés il y a environ 10 ans dans le *New Yorker*. La plupart des affaires citées dans cette série, à l'époque, n'avaient rien à voir avec les infractions relatives aux ordinateurs en que telles, mais démontraient tout simplement l'absence de sens commun, de bonne administration—par exemple, l'absence de système de contrôle et de vérification distinct du système de comptabilité ne permettant pas une vérification indépendante.

Dans une banque, il y a dichotomie entre les programmeurs, les concepteurs de logiciel et les utilisateurs des systèmes ainsi réalisés. C'est un principe administratif tout à fait ordinaire. D'une manière plus générale, dans une banque ou dans une institution financière, ou même, d'ailleurs, dans une entreprise, un bon système de contrôle implique la séparation des services de comptabilité de ceux de Vérification, ce qui n'est pas le cas dans les affaires d'infractions relatives aux ordinateurs.

Certains livres écrits au Canada et certains articles considèrent les infractions relatives aux ordinateurs comme un problème sérieux. Par exemple, dans ces livres sur les banques, Mme Granger agite l'épouvantail des infractions relatives aux ordinateurs au Canada. En réalité, toutes les affaires qu'elle cite sont américaines. Elle ne cite aucune affaire canadienne.

Je me permettrai de vous citer un article publié récemment, le 25 avril 1983 dans le *Globe and Mail*. Dans cet article, le professeur Anne Kittler du *Ryerson Polytechnical Institute* parle des invasions de la vie privée provoquées par les ordinateurs, et je voudrais simplement vous citer un ou deux exemples de propos pouvant grandement induire en erreur le public.

Dans cet article, elle dit:

Dans une institution financière locale, un programmeur a déposé dans son propre compte les fractions de cents créées par les calculs d'intérêt et a amassé très rapidement près de \$100,000.

Ce paragraphe est rédigé dans un contexte pouvant faire penser que cela s'est passé au Canada. Cela n'est jamais arrivé au Canada, c'est arrivé aux États-Unis il y a 15 ans. C'est toujours l'exemple cité, le prototype de l'infraction relative aux ordinateurs où quelqu'un multiplie le prélèvement d'une petite somme auprès d'un grand nombre de sources afin d'en tirer profit.

C'est une vieille histoire rabâchée qui est arrivée il y a longtemps. Je n'en connais pas les circonstances exactes mais ce n'était pas certainement au Canada.

Dans le paragraphe suivant, elle dit:

L'été dernier, nous avons appris que la Banque de Commerce canadienne impériale s'était fait subtiliser près de 10 millions de dollars en deux ans par un employé qui, grâce à

[Text]

over two years by an employee who used the computer and set up phony loans and deposited the money in his account.

Well, that employee certainly did not use a computer. My guess is that employee did not even know how to use a computer—there was no computer involvement whatsoever. It was a straight out and out matter of dealing with the written ledgers in the branch and that sort of thing. It had nothing to do with computers at all. But this was written by a woman who professes to be a specialist in computer sciences. That demonstrates the extent to which the problem is blown out of proportion by stories in the press.

I want to summarize the conclusions that we have come to, Mr. Chairman, and perhaps then we will be able to deal with your observations and questions.

First of all, we believe that internal control mechanisms can be used to reduce the risk of unauthorized activity in a computer environment. This is at the bottom of page 12 of our brief. In fact, if you wish to explore that, we will be glad to enlarge on that, but all banks in this country have very extensive internal control systems. We have a gentleman here representing one of the banks who specializes in that activity and we would be happy to talk about it.

• 0955

Our second point is that computer crime is a misnomer. If the various abuses generally subsumed under this heading are carefully analysed, it becomes clear that true computer abuse comprises only a very narrow field of activity. As the nature of this activity is analogous to existing crimes, true computer abuses might be an appropriate subject for criminal legislation. What we are saying in general is that most offences are, in fact, covered by existing criminal law and by case law.

Our third point, however, is that information abuses deserve careful study, having regard to all the legal vehicles, criminal and non-criminal, available, and to the various existing laws which will be affected. Information must not be separated into computerized and non-computerized information, as this approach places more emphasis on the technology involved than on the action to be deregulated.

The Department of Justice is urged to deal with data in the context of a broader information policy and outside of its proposed bill on computer crime. What we are trying to say here is that the Department of Justice seems to be wanting to deal with data arising from a computer environment rather than data in general. We do not understand the reason for that. We believe that if a bill is going to be developed dealing with criminal access to data and information in general, then it should be a generalized bill of which computer data is only one forum.

[Translation]

l'ordinateur s'était accordé des prêts bidons et avait déposé l'argent dans son compte.

Cet employé ne s'est certainement pas servi d'un ordinateur. Je croirais que cet employé ne savait même pas comment se servir d'un ordinateur—cela n'avait absolument rien à voir avec l'informatique. C'était un simple jeu d'écriture. Cela n'avait rien à voir avec des ordinateurs. Cependant, c'est ce qu'écrit une femme qui professe être spécialiste en informatique. Cela est indicatif du gonflage disproportionné de ces histoires rapportées par la presse.

J'aimerais maintenant résumer nos conclusions, monsieur le président, puis nous pourrions passer à vos questions.

Premièrement, nous croyons que les mécanismes de contrôle interne peuvent réduire le risque d'activité illégitime dans un environnement informatisé. Cette conclusion se trouve au haut de la page 13 de notre mémoire. En fait, si cette question vous intéresse, nous ferons un plaisir d'en discuter plus longuement, mais toutes les banques de ce pays ont des systèmes de contrôle interne très poussés. Nous avons parmi nous le représentant d'une des banques dont cette activité est la spécialité et c'est avec plaisir que nous en discuterons.

Deuxièmement, nous estimons que l'expression «infraction relative aux ordinateurs» est vraiment inappropriée. Lorsqu'on fait l'analyse des divers «délits» qui se rangent sous cette appellation, il devient évident que les infractions réelles relatives aux ordinateurs correspondent à un nombre minime d'activités. Ces dernières étant par leur nature analogue à d'autres déjà cataloguées comme criminelles, il est logique de suggérer que les infractions réelles contre l'ordinateur soient couvertes par une législation criminelle appropriée. Nous disons en substance que la majorité de ces délits sont déjà couverts par les législations criminelles existantes.

Troisièmement, nous estimons cependant que le problème des infractions relatives à l'information mérite d'être étudié avec beaucoup de soins, eu égard à tous les véhicules légaux, criminels et non-criminels, disponibles et aux lois existantes qui pourraient être mises en cause. L'information ne doit pas être compartimentée en données informatisées et non informatisées, car pareille approche met l'accent sur la technologie plutôt que sur l'activité elle-même.

Nous demandons au ministère de la Justice de placer les données dans le contexte d'une politique plus large sur l'information et de les exclure de son projet de loi sur les infractions relatives aux ordinateurs. Il nous semble que le ministère de la Justice veuille ne considérer les problèmes relatifs aux données que dans le cadre d'un environnement informatisé et non pas dans un cadre général. Nous n'en comprenons pas la raison. Nous croyons que si un projet de loi doit traiter de l'accès criminel à des données et à des informations en général, il devrait être plus général et les données informatisées devraient n'être qu'une partie parmi tant d'autres.

[Texte]

And our last point is that the institution of mandatory reporting of computer-related crimes is not justified and would be a major departure in Canadian legal practice.

Mr. Chairman, in addition to these general conclusions, perhaps you would be interested if I were able to table a brief we presented to a Senate committee two weeks ago on the laws of evidence, because those do have some connection with the issues before you. I have copies in English and French of the brief we presented at that time to the Senate committee and also of the Hansard proceedings of the Senate at that time. We did touch briefly in that committee of the Senate on the issue of computer crime, but basically we did not bring along with us here today the individuals who are best qualified to deal with that subject. I would have to beg off dealing with those issues on account of the fact we did not bring with us the legal experts who are best qualified to deal with that. But we would, with your permission, like to table that brief.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): We would be pleased to have a copy of the brief and any other notes and information you might have that would be helpful.

Mr. MacIntosh: Thank you, Mr. Chairman. That is all I have now.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Probably including the article that you spoke from, as well.

Mr. MacIntosh: Yes, sir, we will xerox this and give it to you, or perhaps...

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): We can have that done now.

Mr. MacIntosh: All right.

Mr. Beatty: Their brief to the Senate committee, it might be useful to append that to our minutes for this morning, because it deals with the evidence provisions...

The Acting Chairman (Mr. Robinson Etobicoke—Lakeshore)): I am not so sure that we want to append to our minutes material that has already been placed on the record before another parliamentary committee, albeit a Senate committee. We can always refer to it if we want to.

Mr. Beatty: I think it is germane. Part of our order of reference and the subject-matter of my bill, of course, deals with the Canada Evidence Act, and the hearings that are going on in the Senate on the Senate legislation are very much germane to the work we are doing here and indeed we will probably be expected later to follow up on that.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I would think that if there is anything that has been presented before the Senate committee that is relevant, it could be referred to by our witnesses, and if they refer to it

[Traduction]

Quatrièmement, nous estimons que l'obligation de rapporter les infractions reliées à l'informatique n'est pas justifiée et constituerait une innovation importante en matière de droit canadien.

Monsieur le président, en plus de ces conclusions générales, il vous intéresserait peut-être que je dépose un mémoire que nous avons présenté au Comité du Sénat chargé d'étudier les lois sur la preuve il y a deux semaines, car il a un certain rapport avec les questions qui vous concernent. J'ai des copies en anglais et en français du mémoire que nous avons présenté à ce Comité du Sénat ainsi que des copies du compte rendu de cette séance. Nous avions brièvement abordé la question des infractions relatives aux ordinateurs, mais nous ne nous sommes pas fait accompagner aujourd'hui des personnes mieux qualifiées pour vous parler de cette question. Je vous demanderais d'éviter ce sujet car nous n'avons pas avec nous nos spécialistes juridiques qui sont les mieux qualifiés pour en parler. Cependant, avec votre permission, nous aimerions déposer ce mémoire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Nous serions heureux d'avoir un exemplaire de ce mémoire et de tout autre document en votre possession pouvant nous aider.

M. MacIntosh: Merci, monsieur le président. C'est tout ce que j'avais à dire.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Y compris l'article que vous avez cité.

M. MacIntosh: Oui, nous le ferons photocopier pour vous, ou peut-être...

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Nous pouvons le faire faire nous-mêmes immédiatement.

M. MacIntosh: Très bien.

M. Beatty: Il pourrait être utile d'annexer au compte rendu de notre séance de ce matin le mémoire qu'ils ont présenté au Comité du Sénat car il porte sur les dispositions de la preuve...

Le président suppléant (M. Robinson Etobicoke—Lakeshore)): Je ne suis pas certain que nous voulions annexer à notre compte rendu des documents qui figurent déjà dans le dossier d'un autre Comité parlementaire, bien qu'il s'agisse d'un Comité du Sénat. Nous pouvons toujours nous y référer si nous le voulons.

M. Beatty: Je pense que c'est apparenté. Une partie de notre ordre de renvoi et l'objet de mon projet de loi, bien entendu, portent sur la Loi sur la preuve au Canada, et les audiences qui se déroulent au Sénat concernant la loi du Sénat sont très apparentées au travail que nous faisons ici et il est fort probable qu'ultérieurement on nous demandera de prendre la suite.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Si ce qui a déjà été dit devant le Comité du Sénat est pertinent, nos témoins peuvent le répéter, et s'ils nous indiquent les pages où cela se trouve, bien entendu, nous

[Text]

specifically, to pages in the documents, then of course we could append it. But other than that, I do not really see that it is relevant, other than for information for the members to have.

• 1000

Mr. Beatty: I believe Mr. MacIntosh indicated that he did not have the officials here.

Mr. MacIntosh: No.

Mr. Beatty: No, you do not so that I do not have to explain about the questioning today, but rather that the material which they presented, there, is obviously germane to our work. It is directly relevant to our order of reference.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, I am not really so sure that it is. They were appearing before the Senate Committee on Legal and Constitutional Affairs, and the Senate is dealing with the Canada Evidence Act, and certainly not with your bill.

Mr. Beatty: Well, I do not want to protract this, but my bill, as you are aware, amends the Canada Evidence Act. Because of the difficulty under the Canada Evidence Act, as it stands today, with the introduction of computer print-outs, and evidence, there is specific provision in my bill, which would amend the Canada Evidence Act. We have had previous testimony from Mr. Gill that the government's approach to this is contained in S-33, as opposed to being contained in computer legislation per se, so that both the government's response, and the CBA's response, to that element of my bill, have been presented through the vehicle of S-33 in the Senate hearing.

You will notice that they refer to the same cases that we have in our supporting material here. For example, *Bell v. Bruce*, and *McMullin*, and so on.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, maybe under the circumstances, we could have these items appended as exhibits to our minutes, today, as the legal and constitutional affairs issue.

Mr. Beatty: Well, I do not think there is any need for the Senate Hansard, as such... That is the brief that they presented.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right. Then the brief, from The Canadian Bankers' Association, on Bill S-33, the Canada Evidence Act, which was their submission made, in May, to the Legal and Constitutional Affairs Committee of the Senate, is an appendix.

All right. And now who of our witnesses wishes to follow on from Mr. MacIntosh?

Mr. MacIntosh: Mr. Chairman, we would prefer to respond to your questions, but if you want a further summary of our position on the legal side, I would invite Ms Learmonth to speak to this.

[Translation]

pourrions alors l'annexer. Néanmoins, je n'en vois pas véritablement la pertinence si ce n'est qu'à titre informatif pour les députés.

M. Beatty: Je crois que M. MacIntosh a indiqué ne pas avoir ses spécialistes avec lui aujourd'hui.

M. MacIntosh: Non.

M. Beatty: Non, et de toute évidence les documents présentés sont apparentés à nos travaux. Ils concernent directement notre ordre de renvoi.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je n'en suis pas véritablement si sûr. Ils ont comparu devant le Comité du Sénat chargé des questions juridiques et constitutionnelles, et le Sénat étudie la Loi sur la preuve au Canada, et certainement pas votre projet de loi.

M. Beatty: Je ne veux pas prolonger le débat, mais mon projet de loi, comme vous ne l'ignorez pas, amende la Loi sur la preuve au Canada. A cause des difficultés que pose la Loi sur la preuve au Canada, sous sa forme actuelle, avec l'introduction d'imprimés, d'ordinateurs et la preuve, il y a une disposition précise dans mon projet de loi qui modifierait la Loi sur la preuve au Canada. M. Gill nous a déjà dit que les propositions du gouvernement à ce sujet étaient contenues dans le bill S-33, et non pas dans la Loi sur les ordinateurs en tant que telle, si bien que la réponse du gouvernement et celle de l'Association du Barreau canadien, à cet élément de mon projet de loi, ont été présentées devant le Sénat dans le cadre de l'étude du Bill S-33.

Vous remarquerez qu'ils citent les mêmes affaires que celles contenues dans nos documents. Par exemple *Bell contre Bruce*, et *McMullin*, et caetera.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans ces circonstances, nous pourrions faire annexer ces documents à notre compte rendu d'aujourd'hui, le fascicule du Comité des questions juridiques et constitutionnelles.

M. Beatty: Je ne pense pas qu'il soit nécessaire d'annexer le compte rendu du Comité du Sénat, en tant que tel... L'important, c'est le mémoire déposé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Nous annexerons donc le mémoire présenté en mai par l'Association des banquiers canadiens devant le Comité du Sénat sur les questions juridiques et constitutionnelles dans le cadre de son étude du Bill S-33 concernant la Loi sur la preuve au Canada.

Très bien. Lequel de nos témoins souhaite maintenant prendre la suite de M. MacIntosh?

M. MacIntosh: Monsieur le président, nous préfererions répondre à vos questions, mais si vous voulez un autre résumé de notre position sur le plan juridique, j'inviterais M^{me} Learmonth à prendre la parole.

[Texte]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, we might as well get all the witnesses making their comments first, and then we can give our questions afterwards. So Ms Learmonth.

Ms Pat Learmonth (Co-ordinator of Communications, The Canadian Bankers' Association): Yes. Well I would be pleased to go through the paper and highlight some of the primary issues. They are, essentially, summarized in the conclusion that Mr. MacIntosh read to you earlier.

The main thrust of this paper is to attempt to look at the various types of activity which are generally, or in the public's mind, referred to as computer crime, and organize them into some kind of form which gives insight into what the actual meat of the activity is. We suggest that there are two types of activities which really are not involved with the technology at all, and probably should not be dealt with as matters of computer abuse per se.

Those two types of activities are activities in which the computer is used as a tool to commit an existing Criminal Code offense, such as where a computer is used to somehow manipulate funds resulting in a theft, for example.

• 1005

The second type of activity would be one in which the computer was used as a tool to deal in an unauthorized manner with information. We would include the acquisition, use, disclosure, alteration or destruction of information under that heading. What we are left with is what we refer to as true computer abuses. These are not intended to include things like destruction of hardware, for instance.

It is generally accepted that cases like that are amply covered by the provisions of the Criminal Code as it exists today. The types of matters which we do feel remain are outlined on page five of our brief. They are: the unauthorized obtaining of time on a computer or use of a computer; unauthorized system penetration and system crashing. System crashing is something which was discussed by the RCMP in their presentation to this subcommittee in some detail. Both the RCMP and the Department of Justice take the position that the mischief provisions of the Criminal Code are sufficient to deal with this type of activity because the essential result of it is that the system becomes unavailable for use by authorized people. We were left with two essential problems: the unauthorized obtaining of time or use of a computer and unauthorized system penetration. And these are the two matters which we feel would be appropriately dealt with by the Criminal Code at the present time. We feel that the information question as a whole is something that should be dealt with in the context of a broad policy.

It is something that has not been addressed to date. We certainly have not had an opportunity to have any kind of input. It is the kind of matter that the Department of Justice has indicated they might deal with later on this fall. We think that this is an appropriate forum for these information questions.

[Traduction]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Il est préférable que nous entendions les commentaires de tous les témoins d'abord puis que nous posions nos questions après. Madame Learmonth.

Mme Pat Learmonth (coordonnatrice des services de communication, Association des banquiers canadiens): Oui. Je me ferai un plaisir de vous signaler les points les plus importants contenus dans notre document. Pour l'essentiel, ils sont résumés dans les conclusions que M. MacIntosh vous a lues un peu plus tôt.

Dans ce document, nous nous efforçons avant tout de déterminer les divers types d'activités qui, d'une manière générale, sont considérés aux yeux du public comme des infractions relatives aux ordinateurs, et de les regrouper de manière à bien les définir. Selon nous, il y a deux types d'activités qui n'ont réellement rien à voir avec la technologie en tant que telle, et qui ne devraient même pas être considérés comme des infractions reliées à l'informatique.

Il s'agit d'activités dans lesquelles l'ordinateur sert d'outil pour commettre un délit déjà cité dans le Code criminel, comme par exemple la manipulation de fonds par l'intermédiaire d'un ordinateur ayant pour résultat un vol.

Le deuxième genre d'activité porte sur l'utilisation de l'ordinateur comme outil d'accès non autorisé à l'information. Nous incluons dans ce genre d'activité l'acquisition, l'utilisation, la divulgation, l'altération ou la destruction d'informations. Il nous reste alors ce que nous appelons les vrais abus d'utilisation de l'ordinateur. Cela n'inclut pas, par exemple, la destruction de l'équipement même par exemple.

D'une façon générale, il est reconnu que de tels cas sont tout à fait prévus dans les dispositions du Code criminel actuel. Les questions qu'il reste à examiner sont présentées à la page 5 de notre mémoire. Il s'agit de: l'obtention non autorisée de temps d'utilisation d'un ordinateur; l'intrusion dans un système; et le dérèglement volontaire d'un système. La Gendarmerie Royale du Canada, lors de sa comparaison devant le présent sous-comité, a parlé d'une façon assez détaillée de ce dérèglement. Et la Gendarmerie Royale et le ministère de la Justice ont adopté la position que les dispositions actuelles du Code criminel relatives aux méfaits suffisent à réglementer ce genre d'activité puisqu'il a pour résultat final de nuire à l'utilisation du système par des usagers légitimes. Cela nous laisse donc deux problèmes fondamentaux: l'obtention non autorisée de temps d'utilisation d'un ordinateur et l'intrusion dans un système. A notre avis, ce sont là les deux points qu'il conviendrait d'intégrer au Code criminel. Nous estimons que la question de l'information, dans son ensemble, serait mieux servie par l'élaboration d'une politique générale.

Jusqu'à présent, on n'a pas examiné cet aspect. Nous n'avons certainement pas eu la possibilité de participer le moins. Le ministère de la Justice a laissé entendre qu'il pourrait s'intéresser à cette question plus tard cet automne. Nous croyons que ce serait là le moyen approprié de s'attaquer aux questions sur l'information.

[Text]

That is the meat of this brief. If you have any specific questions about the individual items, we would be pleased to answer them.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): All right. Are there any others who wish to make a contribution at this time, or shall we start on the questioning?

Mr. MacIntosh: We have no further contributions, Mr. Chairman.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Let the record show, then, that Mr. Beatty moved that the item entitled "The Submission to the Senate Committee on Legal and Constitutional Affairs by the Canadian Bankers Association" be appended to our minutes today.

All right, Mr. Beatty, would you like to commence the questioning?

Mr. Beatty: Thank you, Mr. Chairman. Mr. MacIntosh, first of all, thank you for coming today. It was an early morning for you in coming up from Toronto, too, so we are doubly grateful for your presence here.

Inevitably, when testimony turns, to an extent, on the question of the extent of computer crime, the obvious question is: on what basis can anyone make an assertion as to whether or not computer crime exists in Canada? You cited a survey that was done, I believe, with the police of reported instances of computer crime. But in your brief, one of the points you stress very strongly is that there should be no mandatory reporting of violations of computer systems. Indeed, there is none today and much of the expert testimony we have had, on one occasion or another, has suggested that institutions such as banks who may have had their security violated may feel that it is bad public relations to have it widely known they have been the victim of a computer crime and that their systems may not be safe.

Have you, in fact, made a comprehensive survey of the members of your association and asked them for instances which have gone unreported to the police where they may not have been aware of the culprit or where internal disciplinary action may have been taken but where no criminal charges were laid?

Mr. MacIntosh: There are two points I would like to make. The first is that we have canvassed the banks, through our committee structure and through the preparation of this brief, to find out if there was any data base at all indicating the existence of computer crime. I have to tell you that there is simply no data because there have been no cases.

• 1010

Of course, the theft of credit cards is a common phenomenon. I am saying that in the context of our brief that is not a

[Translation]

Voilà le fond de notre mémoire. Si vous avez la moindre question précise sur des aspects particuliers, nous serions heureux d'y répondre.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Très bien. Est-ce que les autres témoins veulent dire quelque chose maintenant ou pouvons-nous commencer les questions?

M. MacIntosh: Il n'y a pas d'autre énoncé, monsieur le président.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Qu'il soit consigné au procès-verbal dans ce cas, que M. Beatty a proposé que le document intitulé «Mémoire présenté au Comité du Sénat de la justice et des questions juridiques par l'Association des banquiers canadiens» soit annexé au procès-verbal d'aujourd'hui.

Très bien, monsieur Beatty, voulez-vous commencer les questions?

M. Beatty: Merci, monsieur le président. Monsieur MacIntosh, tout d'abord, je vous remercie d'être venu aujourd'hui. Vous avez dû vous lever bien tôt pour venir de Toronto et donc nous vous sommes d'autant plus reconnaissants de votre présence ici.

Inévitablement, jusqu'à un certain point, les témoignages tournent autour de l'étendue du crime par ordinateur et donc la question évidente à poser c'est: sur quoi peut-on se fonder pour affirmer s'il y a ou non des crimes par ordinateur au Canada? Vous citez une enquête effectuée, je crois, par la police, sur les cas rapportés de crimes par ordinateur. Toutefois, dans votre mémoire, un des points que vous accentuez très fortement, c'est qu'il n'existe aucune obligation de faire rapport d'intrusion dans un système d'informatique. En fait, il n'en existe aucune aujourd'hui, et une grande partie des témoignages d'experts que nous avons entendus, à un moment ou à un autre, laisse supposer que les institutions telles que les banques dont la sécurité a pu être violée estiment qu'il serait de mauvaise presse de faire savoir à tous qu'elles ont été victimes d'un crime par ordinateur et que leurs systèmes ne sont peut-être pas sûrs.

Avez-vous, en fait, effectué une enquête approfondie auprès des membres de votre association pour leur demander, par exemple, quels crimes n'ont pas été rapportés à la police, soit parce qu'ils ne savaient pas qui était le coupable, soit parce qu'ils ont pris des mesures disciplinaires internes, mais sans qu'il n'y ait d'accusation criminelle?

M. MacIntosh: Je tiens à faire valoir deux points. Tout d'abord, nous avons pris des renseignements auprès des banques, soit par l'entremise de notre comité, soit lors de la préparation du présent mémoire, afin de savoir s'il y avait la moindre donnée qui permette de croire qu'il y a des crimes par ordinateur. Je dois vous dire qu'il n'y a aucune donnée, tout simplement parce qu'il n'y a aucun cas.

Évidemment, le vol de cartes de crédit est assez commun. Si je le dis, c'est dans le contexte de notre mémoire, car il ne

[Texte]

computer crime; that is an ordinary theft. If you steal a person's wallet which includes some credit cards, that is an ordinary theft. The improper use of the card to access the purchase of goods or to access a cash dispenser machine is a form of theft. It is not very different from walking behind the counter in the branch and taking the cash out. It is a different vehicle for doing it, but it is not different as a crime.

We have said in our brief that whether you commit murder with a gun or with a knife is a question of defining the methodology but not the crime itself. The crime is the murder.

We do not have any data base showing that there have been computer crimes.

With regard to covering up, this is a fairly common perception which we think is around that the fact that there is no data base must prove that we are trying to hide something. That is not the case. The fact is that there is nothing to hide.

It is true that there are from time to time embezzlements in banks and defalcations, frauds of various sorts involving bank employees. The banks deal with those on an ad hoc basis, and from time to time they are serious enough to warrant calling in the police. But the fact is that we have not had any computer crimes that would warrant any investigation... There have not been any, in fact, so there has been nothing that one could refer to the police.

Mr. Beatty: By definition you appear to rule out anything that involves either fraud or theft as computer crime as such; you would set that aside in a different category.

Mr. MacIntosh: That is right because I am saying that is an ordinary criminal offence taken care of by the existing criminal law.

Mr. Beatty: Whereas when other people refer to computer crime their inclination would be to include... If the computer was used as a vehicle for the crime, they would tend to include that as computer crime as well. So there is a question of definition to an extent.

Mr. MacIntosh: The issue at stake is whether or not it is necessary to develop new legislation to deal with that offence.

Mr. Beatty: I guess there were two issues. One was the assertion that there has been no computer crime as such, and I suppose it depends what you consider to be computer crime. By your definition there would be three areas which you would feel were appropriate perhaps: First, the unauthorized obtaining of time on a computer; second, unauthorized system penetration; and, third, system crashing. Are you saying to the committee that there is no instance among any of your members where an individual has had unauthorized obtaining of time on a computer?

Mr. MacIntosh: That is right; we have no cases like that.

Mr. Beatty: No instances. There have been no disciplinary actions taken by any of your members against employees who have improperly used facilities?

[Traduction]

s'agit pas d'un crime par ordinateur; il s'agit d'un vol ordinaire. Si vous volez un portefeuille dans lequel se trouvent des cartes de crédit, c'est un vol ordinaire. L'utilisation frauduleuse de la carte afin de se procurer des biens ou pour obtenir l'accès à une distributrice d'argent, c'est encore une forme de vol. Ce n'est pas très différent de faire le tour du comptoir dans une succursale bancaire et de prendre l'argent. C'est un moyen différent, mais le crime n'est pas différent.

Nous avons déclaré dans notre mémoire que le fait de commettre un meurtre avec une arme à feu ou avec un couteau demande qu'on définisse la méthode mais non le crime même. Le crime, c'est un meurtre.

Nous n'avons aucune donnée qui démontre qu'il y a eu des crimes par ordinateur.

Quant à cacher la chose, c'est là une idée assez commune, à savoir que s'il n'y a aucune donnée c'est parce que nous tentons de cacher quelque chose. Ce n'est pas le cas. Le fait est qu'il n'y a rien à cacher.

Il est vrai que de temps à autre, des employés des banques détournent des fonds de la banque ou s'adonnent à des fraudes de diverses sortes. Les banques s'en occupent d'un façon ponctuelle, et de temps à autre, ces agissements sont suffisamment graves pour faire appel à la police. Toutefois, le fait est que nous n'avons eu aucun crime par ordinateur qui justifie une enquête... Il n'y en a pas eu en fait, donc il n'y a eu rien pour lequel on puisse faire appel à la police.

M. Beatty: Par définition, vous semblez écarter de la définition d'un crime par ordinateur tout ce qui se rapporte aux fraudes ou aux vols; vous en faites une catégorie différente.

M. McIntosh: En effet, car il s'agit là d'une infraction criminelle ordinaire assujettie au droit criminel actuel.

M. Beatty: Alors que lorsque d'autres parlent de crime par ordinateur, ils sont portés à inclure... Si l'ordinateur a servi d'outil pour le crime, ils ont tendance à en faire un crime par ordinateur. Donc il s'agit jusqu'à un certain point d'une question de définition.

M. McIntosh: La question à l'étude est de savoir s'il faut ou non mettre au point une nouvelle loi dans le cas de ce délit.

M. Beatty: Je suppose qu'il y avait deux questions. D'abord votre affirmation qu'il n'y a eu aucun crime par ordinateur comme tel, et je suppose que cela dépend de votre définition de crime par ordinateur. Selon votre définition, vous estimez qu'il convient peut-être d'y inclure trois domaines: d'abord, l'obtention non autorisée de temps d'utilisation de l'ordinateur; deuxièmement, l'intrusion dans un système; et enfin, l'intrusion dans un système afin de le dérégler. Nous dites-vous qu'il n'y a eu, parmi vos membres, aucun cas de quelqu'un qui obtienne d'une façon non autorisée du temps d'utilisation d'un ordinateur?

M. McIntosh: En effet; nous n'avons rien vu de semblable.

M. Beatty: Aucun cas. Aucun de vos membres n'a pris de mesures disciplinaires à l'endroit d'employés qui ont fait un usage abusif des installations?

[Text]

Mr. MacIntosh: That is right.

I should point out that we have preventive systems in the computer operations which make it very difficult to do that. The preventive systems have to do with access control.

For instance, in the banking system in Canada today there are about 30,000 terminals in the branches, and likewise in other financial institutions there are also terminals, in the *caisses*, the credit unions, the trust companies and so forth. To get onto that terminal requires having a key and having the code which accesses from the terminal to the data base, and that is simply not available. There is in effect a password system which gives access to the computer by an authorized person. You cannot walk in off the street and make a terminal work for you. It does not work that way.

The next level of control is that there are very extensive software systems to perform checks and controls, internal audit and control systems which are highly developed now. I would have to say that the audit and control that you can apply to financial data with the use of computers is far more extensive than it would have been by hand.

• 1015

A clerk going over paper ledgers and records is a lot slower and more inefficient than a computer scanning data. Every bank in this country, I am sure, or most banks, would have systems where each morning the branch manager, on his desk, has a print-out which shows the transactions for the preceding day with exception performances. He can scan that sheet; and if he sees that an account which has been inactive for three months is suddenly very active, it is going to be drawn to his attention immediately. If he had been trying to do that in the old days by a manual method, he never would have spotted it at all. But the great merit of the computer is that you can retrieve information at such speed and you can also control it; and therefore, you can study what you have. I would say both the accuracy and the obstacles to fraudulent use of data are far greater than they were before the time of computers.

Mr. Beatty: So you say there has been not a single instance that any of your members has had with unauthorized obtaining of time.

Mr. MacIntosh: That is right, none that we know of.

Mr. Beatty: Not a single instance of unauthorized system penetration.

Mr. MacIntosh: That is right. I do not know of a single case. There is one case we identified through one of the police forces. It was a minor case, where I believe a teller acquired perhaps \$5,000. Having left the employment of the institution, the teller got back and somehow get a few thousand dollars. We do not have the details from the police who were involved in the case. That is the only one we know of.

[Translation]

M. McIntosh: En effet.

Je dois souligner que nous avons des systèmes préventifs qui rendent très difficile l'accès non autorisé à nos ordinateurs. Ces systèmes portent sur le contrôle à l'accès.

Par exemple, dans le réseau bancaire au Canada aujourd'hui, il existe environ 30,000 terminaux dans les succursales, en plus de ceux dans les autres institutions financières, dans les caisses, les *credit unions*, les sociétés de fiducie, etc. Pour obtenir accès au terminal, il faut une clé et un code qui permettent à partir du terminal d'avoir accès à la base de données, et cela n'est tout simplement pas disponible. Il existe en fait des mots de passe qui permettent au personnel autorisé d'avoir accès à l'ordinateur. Vous ne pouvez pas vous amener comme ça de but en blanc et faire fonctionner le terminal. Ce n'est pas ainsi que cela fonctionne.

Il existe en outre un autre niveau de contrôle constitué par des logiciels très coûteux qui effectuent des vérifications et des contrôles, une vérification interne en plus de systèmes de contrôle qui sont maintenant très perfectionnés. En outre, la vérification et le contrôle qu'on peut exercer sur les données financières grâce aux ordinateurs sont beaucoup plus poussés que ce qui était possible à la main.

Un commis qui fait la lecture de pages de grands livres et de dossiers va beaucoup plus lentement et moins efficacement qu'un ordinateur qui balaie des données. Chaque banque, au pays, j'en suis persuadé, ou la plupart des banques ont en place un système qui veut qu'à chaque matin le directeur de la succursale ait sur son bureau un imprimé d'ordinateur où figurent les transactions de la veille et les transactions exceptionnelles. Il peut balayer la feuille du regard; s'il constate qu'un compte inactif depuis trois mois est tout à coup très actif, son attention s'y trouve attirée immédiatement. S'il avait essayé de le faire par le passé, à la main, il ne l'aurait jamais relevé. Toutefois, le grand mérite de l'ordinateur, c'est qu'il permet d'extraire des données à très grande vitesse et se prête également à un contrôle; par conséquent, vous pouvez étudier ce que vous avez. Je dirais que la précision des données et les obstacles à leur utilisation frauduleuse sont beaucoup plus grands qu'avant l'époque des ordinateurs.

M. Beatty: Donc, vous prétendez qu'il n'y a pas eu un seul cas où l'un de vos membres aurait eu des problèmes avec l'utilisation non autorisée du temps d'ordinateur.

M. MacIntosh: En effet, pas à notre connaissance.

M. Beatty: Pas un seul cas d'intrusion non autorisée.

M. MacIntosh: En effet. Je ne connais pas un seul cas. Il y a eu un cas que nous avons trouvé grâce à l'aide des forces policières. Rien du tout, il s'agissait d'un caissier qui a mis la main sur peut-être 5,000 dollars. Après avoir laissé l'emploi de la banque, le caissier était revenu et avait réussi, d'une façon ou d'une autre, à obtenir quelque milliers de dollars. La police ne nous a pas fait part des détails de l'affaire. C'est le seul cas que nous connaissons.

[Texte]

Mr. Beatty: Then again, you would not consider someone who has used an automated teller machine to get into the system. Because that would be fraud, you would not consider that unauthorized system penetration by your definition.

Mr. MacIntosh: No, I would just call that ordinary fraud.

Mr. Beatty: There is not a single case of system crashing of which your members are aware.

Mr. MacIntosh: No, I do not think so. Perhaps I might ask Mr. Jestin to concur on that. A deliberate bringing down of the system . . .

Mr. Beatty: Yes. My experience with my bank is that it is down a good portion of the time, whenever I am making a withdrawal or a deposit.

Mr. E. (Ted) Jestin (Supervisor, Internal Control Evaluation, The Bank of Nova Scotia, The Canadian Bankers' Association): That is very seldom deliberate.

Mr. MacIntosh: With regard to down time, if I could comment on that, down time is always a concern of financial institutions. The truth is that down time occurs mostly on Friday noon before a long holiday weekend. There is a reason for that. The systems were built to handle certain peak-load levels, as a hydro-electric power system is; and sometimes your transaction volumes can go right off the top of the chart, and you do get problems in that case.

It is very difficult to build a degree of redundancy that prevents that from ever happening; but the fact is that down time in the Canadian banking system is less than 1% right now, which is a very low figure. It has a very high degree of reliability compared to other computer systems in Canada. If you compare it to the stock exchange, for example, our reliability is far higher than theirs or the department stores', or for that matter, the government computers.

You can get down time for all kinds of reasons. One of the most common would be that the telecommunications cables get broken. I have personally experienced cases where a construction worker with a backhoe cut through a major cable outside Toronto, and it took down the whole computer system of all the banks. That kind of case, of course, to the customer at the desk appears to be a computer failure. In fact, it was the telephone people's failure.

Mr. Beatty: I think perhaps, for the record, I should clarify one point. One thing disturbs me. I agree with you, certainly, that computerization can lead to much greater security. It certainly leads to a provision of a range of services which were completely beyond comprehension prior to computers.

My purpose in introducing legislation was not to delay computerization or to in any way inhibit the ability of institutions to computerize; but rather, my great fear is a complacent self-satisfaction on the part of institutions which

[Traduction]

M. Beatty: Encore une fois, vous ne tenez pas compte de quelqu'un qui se servirait d'un guichet automatique pour gagner accès au système, puisqu'il s'agirait là d'une fraude, selon votre définition, il ne s'agirait pas d'une intrusion non autorisée.

M. MacIntosh: Non, j'appellerais cela une fraude ordinaire.

M. Beatty: À la connaissance de vos membres, il n'y a pas eu un seul cas de mise en panne d'un système.

M. MacIntosh: Non, je ne le crois pas. Je peux peut-être demander à M. Jestin de le confirmer. La mise en panne délibérée du système . . .

M. Beatty: Oui. À ma banque, j'ai constaté que l'ordinateur est en panne souvent, lorsque je fais un retrait ou un dépôt.

M. E. (Ted) Jestin (surveillant, Évaluation des contrôles internes, Banque de Nouvelle-Écosse, Association des banquiers canadiens): C'est très rarement à dessein.

M. MacIntosh: Pour ce qui est des pannes, si vous voulez bien me permettre quelques commentaires à ce sujet, ces pannes préoccupent toujours les institutions financières. La vérité, c'est que les pannes se produisent la plupart du temps le vendredi midi, avant une longue fin de semaine. Mais cela s'explique. Les systèmes ont été construits pour faire face à certaines charges de pointe, tout comme le réseau hydro-électrique; parfois, le volume de vos transactions monte en flèche et, alors, vous avez des problèmes.

Il est extrêmement difficile de prévoir suffisamment de redondance pour empêcher que cela ne se produise jamais; toutefois, le fait est que les périodes de panne dans le réseau bancaire canadien ne représentent que moins d'un p. 100 à l'heure actuelle, un chiffre très faible. Nos ordinateurs sont très fiables comparés aux autres réseaux d'ordinateurs au Canada. Si vous comparez par exemple à la bourse, nos ordinateurs sont beaucoup plus fiables que les leurs ou ceux des grands magasins ou même, à bien y penser, ceux du gouvernement.

Vous avez des pannes pour toutes sortes de raisons. La plus commune, c'est le bris des câbles de télécommunication. J'ai personnellement eu connaissance d'un cas où un ouvrier en construction avec sa rétrocaveuse avait percé un des câbles principaux à l'extérieur de Toronto, ce qui avait mis en panne tout le réseau d'ordinateurs de toutes les banques. Pour le client au comptoir de la banque, il semble s'agir d'une panne d'ordinateur. En fait, c'était la compagnie de téléphone qui était en défaut.

M. Beatty: Je crois que je dois préciser une chose, pour que le procès-verbal soit clair. Une chose m'ennuie. Je conviens avec vous, certainement, que l'informatisation peut entraîner une bien plus grande sécurité. Cela a certainement permis toute une gamme de services tout à fait impensables avant les ordinateurs.

Si j'ai présenté ce projet de loi, ce n'était pas afin de retarder l'informatisation ou de gêner le moins possible les institutions qui veulent adopter l'ordinateur; au contraire, ma plus grande crainte, c'est de voir les institutions qui ont des

[Text]

have computers that it cannot happen here and there really is no problem. That was clearly in place prior, for example, to the Dalton school incident, where a number of computer systems in Canada were attacked and some were, in fact, successfully invaded from New York City. That sort of incident and the attending publicity is apt to lead to reaction both by government and by the public, which could have very Draconian sweeping legislation. That could certainly seriously impede the ability of institutions to use computers, and to provide the range of services that we have come to take for granted.

• 1020

The purpose for posing legislation and for urging that the committee have hearings at this point, was that it should be in a moment of calm and relative peace when we consider legislation like this rather than during a panic reaction after "the big incident" has taken place, and we have found that tens of thousands of people's personal records have spewed out through someone's apple tree, or that the accounts receivable of a company have been lost and they are forced to close their doors or to lay off employees as a result.

I just think it is important to indicate that both the committee's motivation and my motivation are not ones of being opposed to computers, or of being afraid of computers. Rather, it is a feeling of it being essential that we lay the legal infrastructure in place now when we are not up against the pressure of an incident of widespread public concern as opposed to over-reacting to some incident that takes place.

Mr. MacIntosh: Well, we agree that there are some issues which should be dealt with in legislation, but we are saying that there is, sort of, a rather narrow spectrum of issues which would not now be covered by existing criminal law.

Mr. Beatty: I am inclined to agree. Can we take a look at those? Could you give me your reaction to the following:

Say the committee were to make a report in which our recommendation to Parliament is that the government should, first of all, introduce legislation dealing with creating an offence similar to mischief, of computer trespass or data trespass, unauthorized access to a computer system, as a first separate bill to be acted on in fairly short order;

that, second, the question of software should be dealt with in the context of revisions to copyright legislation, and not in a computer statute as such;

third; that an investigation should be made of trade secrets legislation to determine whether or not it is up to speed with contemporary realities;

fourth; that at a later date the question of data security standards for institutions holding information about individuals, should be looked at but, at this point, we have not had sufficient experience in the government sector so that we could apply standards to the private sector;

[Translation]

ordinateurs se complaire à croire que cela ne peut pas se produire chez elles et qu'il n'y a vraiment aucun problème. C'était certainement l'attitude qui prévalait, par exemple, avant l'incident de l'école Dalton au cours duquel plusieurs réseaux d'ordinateurs au Canada ont été attaqués avec succès à partir de New York. Ce genre d'incidents et la publicité qui s'y rattache risquent d'entraîner des réactions à la fois de la part du gouvernement et du public qui pourraient entraîner la mise en place d'une loi générale très draconienne. Cela gênerait gravement, certainement, la capacité des institutions à se servir d'ordinateurs et à offrir toute la gamme des services que nous trouvons maintenant tout naturels.

Le but de proposer une loi et de prier le Comité de tenir des séances maintenant, c'était justement que nous connaissions une période assez calme pour étudier un tel projet de loi plutôt que de le faire en réaction à un «grand incident» où on constaterait, par exemple, que des dizaines de milliers de dossiers personnels ont été éparpillés ou que les comptes recevables d'une entreprise sont perdus et que celle-ci a dû fermer ses portes ou licencier ses employés, suite à cette perte.

Je crois qu'il est important de préciser que la motivation qui anime le Comité et qui m'anime n'a rien à voir avec une opposition aux ordinateurs ou à la crainte des ordinateurs. Plutôt, c'est qu'il est essentiel que nous mettions en place maintenant une infrastructure légale lorsque nous ne sommes pas poussés par un incident qui toucherait de près le public et qu'on ne risque pas de trop réagir à quelque chose qui s'est produit.

M. MacIntosh: Nous convenons que certaines questions doivent faire l'objet d'une loi, mais nous tenons à préciser que peu de questions ne sont pas déjà assujetties au droit criminel actuel.

M. Beatty: Je suis porté à en convenir. Pouvons-nous examiner ces aspects? Pouvez-vous me dire ce que vous pensez de ce qui suit.

Disons: que le Comité publierait un rapport dans lequel nous recommanderions au Parlement que le gouvernement devrait, tout d'abord, présenter un projet de loi portant sur les infractions semblables à celle de méfait, d'intrusion dans les ordinateurs ou d'indiscrétion en matière de données, d'accès non autorisé à un système d'ordinateurs, le tout dans un projet de loi séparé à présenter à assez brève échéance;

que, deuxièmement, la question du logiciel soit examinée dans le contexte de la révision de la Loi sur les droits d'auteur et ne figure pas comme telle dans une loi sur les ordinateurs;

troisièmement, qu'on fasse une étude des lois sur les secrets commerciaux afin de voir si celles-ci ont gardé le pas par rapport aux réalités contemporaines;

quatrièmement, que, plus tard, on étudie la question des normes de sécurité pour les données confiées à des institutions qui entreposent de telles données sur les individus, mais que, pour l'instant, nous n'avons pas suffisamment d'expérience

[Texte]

fifth; that it would be very useful if, in the educational process in universities among computer science courses being taught, that computer ethics should also be taught as well simply how to use the system. What would be your reaction to recommendations similar to that? With which ones would you quarrel? Or would you feel that would be a useful report to make?

Mr. MacIntosh: I will ask Ms Learmonth, who is a lawyer and I am not, to address the first several of those.

Ms Learmonth: Maybe I will not start with No. 1; I will start with No.2 and No.3, insofar as taking a look at the copyright legislation and looking at the possibility of dealing with software in that context—reviewing the law of trade secrets. From a legal point of view, that makes a great deal of sense. I do not think we would have any problem with that. I think we clearly support that approach in our brief.

On the question of whether there should be some additional legislative provision in terms of data security standards. If I interpret what you are saying correctly, you are suggesting that a piece of legislation be put in place which would legislate data security standards. Is that . . .

Mr. Beatty: No. I was saying that the government may look at that at some point, but we are not in a position to recommend that such legislation be put in place at the present time. However, clearly there is a concern where institutions hold information relating to the personal affairs of individuals in particular, and that this is clearly an area where more study is needed.

Ms Learmonth: From the point of view of the banks in particular, I would respond to that by saying that there is a large number of legal restraints on the banks at the present time in terms of confidentiality and the maintaining of bank records.

• 1025

You may have reference to Section 157 of the Bank Act to which we referred in our brief and also to, in common law, the Fournier case, which is the foundation case in this area. In addition, of course, there is provincial legislation which deals with confidentiality and credit and so on and so forth. The banks are subject to a large number of provisions dealing with confidentiality and bank records at the present time. I do not think that an additional piece of legislation would have a significant impact on the banks . . .

Mr. Beatty: . . . On the banks, but it would on other institutions.

Ms Learmonth: . . . on other institutions. I leave that up to other people to comment on.

On your question of education and ethics, it would seem to me that this would make a great deal of sense. It is also referred to specifically in our brief. We feel that as time goes on, ethics and internal controls will be ways in which we can

[Traduction]

dans le secteur gouvernemental qui nous permette d'appliquer des normes au secteur privé;

cinquièmement, qu'il serait très utile, dans les universités, dans le cadre des cours en informatique, qu'on enseigne également la moralité en matière d'ordinateur en plus de la simple utilisation des systèmes. Quelle serait votre réaction à de telles recommandations? Lesquelles voulez-vous contester? Pensez-vous que ce serait là un rapport utile?

M. MacIntosh: Je vais demander à M^{me} Learmonth, qui est avocate, ce que je ne suis pas, de répondre aux quelques premiers points.

Mme Learmonth: Je ne vais pas commencer par le n° 1; en fait, je vais commencer par répondre aux n° 2 et 3, une révision des lois sur les droits d'auteur et la possibilité d'inclure dans ces lois des dispositions sur le logiciel . . . ainsi que la révision de la Loi sur les secrets commerciaux. D'un point de vue juridique, c'est tout à fait sensé. Je ne crois pas que cela nous cause le moindre problème. Je crois d'ailleurs que nous appuyons clairement une telle approche dans notre mémoire.

Quant à savoir si l'on doit prévoir d'autres dispositions législatives sur les normes de sécurité en matière de données, si j'ai bien interprété vos paroles, vous proposez la mise en place d'une loi qui prévoit des normes de sécurité en matière de données. C'est-à-dire . . .

M. Beatty: Non. Je disais que le gouvernement étudiera peut-être cet aspect un de ces jours, mais que nous ne sommes pas en mesure de recommander la mise en place d'une telle loi à l'heure actuelle. Toutefois, le cas des institutions détentrices de renseignements sur les affaires personnelles crée certainement des préoccupations et il est clair qu'il faudra étudier ce domaine de plus près.

Mme Learmonth: Du point de vue tout particulièrement des banques, je puis vous dire que les banques sont déjà assujetties à un grand nombre de contraintes légales en matière de confidentialité et de maintien des dossiers.

Songez notamment à l'article 157 de la Loi sur les banques dont nous parlons dans notre mémoire ainsi que, en droit commun, à l'affaire Fournier, le précédent dans ce domaine. En outre évidemment, il existe des lois provinciales qui portent sur le caractère confidentiel de données et sur le crédit etc., etc.. Les banques sont assujetties à un grand nombre de dispositions à l'heure actuelle portant sur le caractère confidentiel des dossiers. Je ne crois pas qu'une autre loi encore aurait une grande portée sur les banques . . .

M. Beatty: . . . sur les banques, mais sur les autres institutions.

Mme Learmonth: . . . sur les autres institutions. Je laisse les commentaires à ce sujet à d'autres.

Quant à votre question sur l'enseignement de la moralité, il me semble que ce serait là tout à fait raisonnable. Nous le mentionnons expressément dans notre mémoire. Nous estimons qu'avec le temps, la moralité et les contrôles internes nous

[Text]

get at the root of the problem, instead of legislating against the problem after it has occurred.

Your first point, however, dealt with the mischief provisions. There is some concern, here, because it would appear that what is being suggested is that the mischief provisions would be extended to include mischief relating to data. This data would be defined in terms of information—am I wrong?

Mr. Beatty: No; I am sorry. I was suggesting that you would perhaps have a new offence of computer trespass or unauthorized access to a computer system. The penalties would be similar to the penalties for mischief. The purpose would be to close off the loophole that exists. At the present time, accessing a computer system is not against the law. It is not covered under the code unless you crash the system.

Ms Learmonth: No. We specifically support this kind of legislation in our brief. We do not have a problem with it. The only problem that arises is if those provisions, those Criminal Code amendments, in the immediate future, were to deal with data in any way.

Mr. Beatty: I think, increasingly, that the vast rate of the testimony we have had before us is that if you get into the definition of information as property, you are raising both legal and moral implications that go well beyond the issue before the committee today. At this point, we are simply not prepared to deal with this. In large part, you can deal with the problem. If an individual is forbidden to get access to your system, he is not able to manipulate the data on the system and it is possible to keep him out. You have served your purpose. It may be that at another time the government may want to take a look at whether information is, in fact, property, and what sort of sanctions you want to put in place there; but you should not single out computer systems as such. The system of storage is not the critical concern.

Mr. MacIntosh: If I could just intervene. One of the problems, of course, we had in preparing this brief was that we have not got an actual bill before us, so we do not know exactly what the intention of the Department of Justice is and how it drafts its proposals. But it is our understanding that the department is leaning towards the thought of dealing with the issue of access to computerized data. We say this is putting the cart before the horse; to be fascinated with access to computerized data is to be specializing in the problem. The more general issue is access to any data. We cannot see that there is much difference between a person going into a filing cabinet and taking the files out and accessing through a terminal into a computer magnetic tape.

Mr. Beatty: I agree. This is why my inclination would be not to make any reference to data at all, but rather, to say that if I were to break into your office and go through your files, I would have been guilty of break and enter, trespass . . . if I had taken any information from there I may have been guilty of

[Translation]

permettront de nous attaquer à la racine du problème plutôt que de légiférer pour régler des problèmes après le fait.

Votre premier point cependant portait sur les dispositions relatives aux méfaits. Cela soulève des inquiétudes, puisqu'il semblerait que ce que l'on suggère, c'est d'étendre les dispositions relatives aux méfaits pour inclure les méfaits visant des données. Ces données seraient définies comme étant de l'information; ai-je tort?

M. Beatty: Non; excusez-moi. Je proposais qu'on pourrait peut-être créer une nouvelle infraction dans le cas de l'intrusion dans un ordinateur ou de l'accès non autorisé à un système d'ordinateur. Les sanctions seraient semblables à celles pour méfaits. C'est afin de combler les échappatoires qui existent. A l'heure actuelle, obtenir accès à un système d'ordinateur ne va pas à l'encontre de la loi. A moins de dérégler le système, ce n'est pas prévu dans le code.

Mme Learmonth: Non. Nous appuyons expressément ce genre de loi dans notre mémoire. Cela ne nous cause pas de problème. Il n'y aurait problème, à notre avis, que si ces dispositions, ces modifications au Code criminel, dans un avenir immédiat, portaient le moindrement sur les données.

M. Beatty: Je crois que de plus en plus, la grande majorité des témoignages que nous avons entendus soutenaient que si nous définissons l'information comme une propriété, on soulèverait ainsi des répercussions légales et morales qui vont bien au-delà de la question à l'étude par le Comité. Nous ne sommes tout simplement pas prêts à nous attaquer à cet aspect maintenant. Dans une large mesure, vous pouvez régler le problème. Si il est interdit à un individu d'obtenir accès à votre système, il ne peut manipuler les données du système et il est possible d'empêcher qu'il y ait accès. Vous avez ainsi réalisé votre objectif. Il se peut que plus tard le gouvernement veuille étudier la question de savoir si en fait, l'information est une propriété, et quelle genre de sanction on veut mettre en place dans ce contexte; mais il ne faudrait pas uniquement viser les systèmes d'ordinateur. L'entreposage n'est pas la grande préoccupation.

M. MacIntosh: Si vous voulez bien me permettre d'intervenir. L'un des problèmes que nous avons manifestement eu en préparant le présent mémoire, c'est qu'il n'y a pas vraiment un projet de loi et donc nous ne savons pas exactement quelles sont les intentions du ministère de la Justice et comment ce dernier va rédiger ses propositions. Toutefois, nous avons cru comprendre que le Ministère penche en faveur de l'idée de s'attaquer à la question de l'accès aux données d'ordinateur. À notre avis, c'est là mettre la charrue avant les boeufs; l'accès aux données d'ordinateur n'est qu'un aspect du problème. La question plus générale porte sur l'accès à toutes les données. Nous ne pouvons pas voir quelle différence il y a entre quelqu'un qui se rend dans un classeur et prend des dossiers et quelqu'un d'autre qui gagne accès grâce à un terminal à une bande magnétique d'ordinateur.

M. Beatty: Je le reconnais. C'est pourquoi je suis plutôt porté à ne pas du tout parler de données, mais plutôt à dire que si j'allais dans votre bureau et que j'examinais vos dossiers, je serais coupable d'effraction, d'intrusion . . . Si j'avais pris la moindre information de votre bureau, j'aurais pu être coupable

[Texte]

theft. On the other hand, if you were to have the information in a data bank with dial and access, I could do essentially the same thing with your computer without having committed any offence, unless I deprived you of the data, unless I crashed the system and deprived you of use of the system. It seems to me that you could have a rough symmetry if you were to have a crime analogous to computer trespass. Unauthorized access to a computer system would be against the law just as unauthorized access to his office is against the law, and you need not make any reference to data as such or what happens. In fact, once the person is there, that is an issue for another day. If you were not authorized to be in the computer system, you should not be there, and the courts would have the right to make a fine, that you were guilty of an offence.

• 1030

Ms Learmonth: That is our position precisely.

Mr. Beatty: Aside from those five points that are suggested, are there other elements that you feel should be recommended by the committee?

Mr. MacIntosh: Could I ask Mr. Jestin to speak to the issue of data security standards . . .

Mr. Beatty: Sure.

Mr. MacIntosh: —because he knows a good deal about this.

Mr. Jestin: I think one of the reasons that The Canadian Bankers' Association is presenting you with no evidence of misuse or abuse of computing is because the banking industry has taken a proactive stance in instituting responsible security measures and access control mechanisms. The RCMP within the federal government has a responsibility to audit data processing installations and they produce several publications which we utilize in aligning our security strategy. So, therefore, we would be very pleased to participate in the development of such standards or such guidelines as may be appropriate. Basically, our response to that question would be that if there is a definite need identified wherein the banking community or any other data processing community has not developed sufficient internal safeguards, and it appears that legislation or guidelines or data security standards are appropriate, we would certainly be prepared to participate in their development.

Mr. Beatty: One of the issues that came up in the testimony yesterday was the insurance of computer systems and of the information contained in them. Do your members insure their computer systems and have they found that it is possible to buy insurance at a reasonable rate, either from the point of view of ensuring that they would be covered if a system crash takes place, which would deprive them of business, or if there are losses that occur as a result of computer abuse of one form or another. I suppose you are insured in terms of theft and such, but in terms of other forms of computer abuse.

[Traduction]

de vol. Par contre, s'il s'agissait d'obtenir des informations d'une banque de données en recourant à une ligne téléphonique pour y gagner accès, je pourrais faire essentiellement la même chose avec votre ordinateur sans avoir commis d'infraction, à moins que je vous prive de ces données, à moins que je ne fasse tomber le système en panne et que je vous prive de son utilisation. Il me semble qu'on pourrait avoir un assez bon parallèle s'il existait un crime semblable à l'intrusion dans un système d'ordinateur. L'accès non autorisé à un système d'ordinateur irait alors contre la loi tout comme l'accès non-autorisé à votre bureau va à l'encontre de la loi; il ne serait pas nécessaire de parler comme tel des données ou de ce qui s'est produit. C'est le fait, que la personne se soit introduite sans autorisation dont on tiendra compte. Si vous n'aviez pas l'autorisation voulue pour vous servir du système d'ordinateur, vous ne deviez pas être là, et les tribunaux auraient le droit de vous reconnaître coupable d'une infraction.

Mme Learmonth: C'est exactement notre position.

M. Beatty: Outre les cinq points proposés, y a-t-il à votre avis d'autres éléments que le Comité devrait recommander?

M. MacIntosh: Puis-je demander à M. Jestin de parler de la question des normes de sécurité en matière de données . . .

M. Beatty: Certainement.

M. MacIntosh: . . . car il est très au courant de cet aspect?

M. Jestin: Je crois que si l'Association des banquiers canadiens ne vous présente aucune preuve de mauvaise utilisation ou d'abus des ordinateurs, c'est que l'industrie bancaire a pris spontanément des mesures en vue de mettre en place des mécanismes de sécurité responsables et des mécanismes de contrôle de l'accès. La Gendarmerie royale détient au sein du gouvernement fédéral la responsabilité de vérifier les installations de traitement de données et a rédigé plusieurs documents que nous avons utilisés pour modeler notre stratégie de sécurité. Par conséquent, nous serions des plus heureux de participer à l'élaboration de telles normes ou de telles directives jugées appropriées. En fait, en réponse à cette question, si l'on relève au sein de la communauté bancaire un besoin précis ou si tout autre secteur de traitement des données n'a pas mis au point des sauvegardes internes suffisantes, et qu'il semble approprié de mettre en place une loi ou des directives ou des normes de sécurité en matière de données, nous serions très certainement disposés à participer à leur élaboration.

M. Beatty: L'une des questions soulevée dans les témoignages hier a été celle de l'assurance des systèmes d'ordinateur et de l'information qui s'y trouve. Est-ce que vos membres assurent le système d'ordinateur ou ont-ils constaté qu'il est possible d'acheter de l'assurance à des taux raisonnables soit pour se protéger si leur système tombe en panne, ce qui les priverait de revenus commerciaux, ou s'ils encouraient une perte à la suite d'un abus quelconque de leur système d'ordinateur? Je suppose que vous êtes assuré contre les vols, etc., mais êtes-vous assuré pour les autres formes d'abus d'ordinateur?

[Text]

Mr. MacIntosh: I think I can address that more in terms of redundancy systems than in terms of insurance. Insurance would not do you much good if you had a million savings accounts on your central magnetic tape files and you had a fire or a terrorist bomb or an earthquake or anything that caused the destruction of your records. You would be in very bad shape and insurance would not do you much good. So what you have to have is back-up and back-up on top of back-up, and that is what the banks have. The banks have elaborate control systems in which daily the files are transferred away from the premises to an off-site secure place; that is a process which goes on constantly.

First of all, you transfer yesterday's records into a secure vault on your own premises, and the day before's records go off-site altogether, so that at any one time a bank has what are called son, father, grandfather files. There have been instances where there have been fires in Canada and those who have been affected have been able to get back-up in an extremely short time—within a day or two they have been operational again.

Now, of course, there are more things than files involved; there are the computer facilities themselves. Increasingly, the Canadian banks have been building back-up facilities, so that in fact they are able to operate at more than one centre. If one centre were to go down, they have now the capability in most of the big banks of transferring the operation to another centre entirely; so to the general public it would not be apparent that anything had been disturbed. I cannot claim that there would be no disruption at all, but there are enormous expenditures to provide redundancy, as there are in hydroelectric power systems, for example, which is the parallel.

Mr. Beatty: Does this mean you do not attempt to insure your systems with private insurance companies in any way? Presumably, hardware you would insure, but . . .

• 1035

Mr. Jestin: Absolutely, from fire or physical damage, certainly.

Mr. Beatty: What about the data, or programs, or loss of service and so on?

Mr. Jestin: Most of the approach of the data processing industry in general has been a self-insuring type of philosophy wherein when the reliance on the computing facility is increased to the point where it becomes critical to the organization, substantial contingency planning and backup measures are undertaken so that you become self-insuring: separating the critical processing between several sites, ensuring that data movement is sufficient to back you up in the event of a contingency, and finally in many cases in the data processing community there is in existence some reciprocal agreement such that you can move your computing workload to another locale if you sustained an outage.

I do not think insurance does you very much good, because it will not react fast enough. It is important to find yourself in some surplus capacity very quickly and so a major installation

[Translation]

M. MacIntosh: Je crois que je dois vous parler plutôt des systèmes de redondance que de l'assurance. L'assurance ne sert pas à grand-chose si vous avez un million de comptes d'épargne d'enregistrés sur votre bande magnétique centrale et qu'il y a un feu ou une bombe de terroristes ou un tremblement de terre ou quoi que ce soit qui détruise vos dossiers. Vous seriez en très mauvaise posture et l'assurance ne vous ferait pas grand bien. Ce qu'il faut, c'est une relève et une relève à la relève, et c'est ce que les banques ont. Les banques possèdent des systèmes de contrôle diversifiés qui permettent de déménager chaque jour des dossiers à un endroit sûr ailleurs; ce processus est constant.

Tout d'abord, vous déménagez les dossiers d'hier à un coffre-fort solide sur vos lieux d'affaires mêmes, et les dossiers d'avant hier quittent les lieux tout à fait et donc à tout moment les banques ont ce que l'on appelle des dossiers fils, pères, grand-pères. On a vu des cas d'incendies au Canada où ceux qui avaient été touchés ont pu remplacer le tout extrêmement vite—et pouvaient fonctionner un jour ou deux plus tard.

Evidemment, il y a autre chose que les dossiers; il y a les installations mêmes. De plus en plus, les banques canadiennes construisent des installations de relève de façon à pouvoir fonctionner à plus d'un centre. Si un centre tombe en panne, les plus grandes banques sont maintenant capables de transférer complètement leurs activités à un autre centre; ainsi le grand public ne se rend pas compte que quelque chose a changé. Je ne peux pas prétendre qu'il n'y a pas eu la moindre interruption, mais il en coûte énormément cher pour prévoir une redondance comme pour le réseau hydro-électrique par exemple, notre pendant.

M. Beatty: Est-ce que cela signifie que vous ne tentez pas d'assurer vos systèmes chez les assureurs privés? On peut présumer que vous allez assurer l'équipement, mais . . .

M. Jestin: Absolument, en cas de feu ou de dégât matériel.

M. Beatty: Mais les données, les programmes ou la perte de service, est-ce assuré?

M. Jestin: D'une façon générale, dans l'industrie du traitement des données on préconise l'auto-assurance; c'est-à-dire que si un organisme compte sur ses installations informatiques au point où elles ont une importance critique, il entreprend alors la planification de mesures d'urgence considérables et il met en place des systèmes de relève de façon à être autonome. Par exemple, le traitement essentiel se fait à plusieurs endroits différents en s'assurant qu'il y a suffisamment de déplacement des données pour pouvoir se sortir d'affaire dans un cas d'urgence et enfin, très souvent, dans le milieu du traitement des données, il existe des ententes de réciprocité qui vous permettent de faire faire le travail par ordinateur ailleurs s'il y a une panne.

Je ne crois pas qu'une assurance vous fasse grand bien puisqu'elle ne permet pas de réagir assez vite. Il est important de trouver très rapidement une capacité supplémentaire et

[Texte]

with tremendous reliance on the computing facilities within the organization, normally provide a tremendous backup and redundancy capability.

Mr. Beatty: The reason for the question was that I wondered to what extent the market will . . . Certainly in the case of the banks the market demands are such that there are strong pressures on you to have adequate security and have proper backup systems.

There is a problem in the case of newspapers. They could not afford to lose a day's publishing if their system were to go down. Some other institutions, where maintenance of the computer system is critical, would have redundancy and would be able to take up the slack very quickly. In other instances, though, it appears as if very little thought has been given by institutions to having any redundancy at all and the first they learn about the deficiency of their system is when the system is penetrated or when there is a crash and it is lost. I wonder to what extent insurance companies might require, if they were insuring the system, that there would be adequate standards of security and adequate standards of redundancy before a claim would be allowed. The testimony yesterday seemed to indicate that this was an area for which by and large it is not practical to buy insurance, that the insurance fees were so high that it simply did not pay.

Mr. MacIntosh: My guess is that it is not practical to insure because there would be a question of insuring the continuity of your business altogether. The banks are probably the most advanced in terms of redundancy of any form of business in the country, excepting possibly the oil companies and the hydro-electric, a few cases of that nature, but in general business in Canada, I would think the banks have spent more money to develop security and redundancy than any other business, and in the case of a separate additional computer facility you could be talking \$50 million to \$100 million for a viable operation, plus staffing it.

I would think that many small businesses in this country do not have anything like effective redundancy or effective ability to get up again. They are perhaps not able to afford the kind of resources involved in that sort of thing, so increasingly you are going in the direction of reciprocal agreements, as Mr. Jestin said, where they can search out in the neighbourhood a configuration of hardware and software which is sufficiently similar that you could get up again.

Where these things happen, it usually turns out that there are problems with software that does not in fact fit; you have to make adjustments to operate, but it can be done. My guess in general is that the answer is that you could not insure for the kind of risks that are at stake.

Mr. Beatty: Probably you would find a dichotomy between large institutions and small institutions; large institutions such as the banks, presumably the airlines, for which the reservation system would be critical, hotels.

[Traduction]

donc une grande entreprise qui repose énormément sur des installations informatiques doit normalement prévoir des tas de systèmes de relève et de redondances.

M. Beatty: Si je pose la question, c'est que je me demande jusqu'à quel point le marché . . . Il est certain que dans le cas des banques, les exigences du marché sont telles qu'elles les forcent à prévoir une sécurité adéquate et des systèmes de relève appropriés.

Il y a un problème dans le cas des journaux. Ils ne peuvent se permettre de perdre une journée de publication si leur système est en panne. Certains autres secteurs, où il est essentiel de faire l'entretien du système d'ordinateur, prévoient des systèmes de relève et pourrait donc se retourner très rapidement. Dans d'autres cas cependant, il semblerait que certaines entreprises aient très peu réfléchi à utiliser la moindre redondance et elles n'apprennent les lacunes de leur système que lorsque celui-ci est utilisé sans autorisation ou lorsqu'il y a une panne et que tout est perdu. Je me demande jusqu'à quel point les compagnies d'assurance exigeraient, si elles assuraient un système, qu'il y ait des normes adéquates de sécurité et de redondances avant de verser une indemnité. Le témoignage d'hier semblait laisser entendre qu'il s'agit d'un domaine où dans l'ensemble, il n'est pas pratique d'acheter de l'assurance, car les primes d'assurance sont si élevées que ce n'est tout simplement pas rentable.

M. MacIntosh: Je suppose qu'il n'est pas pratique de souscrire une assurance tout simplement parce qu'il faudrait assurer la capacité à continuer les affaires. Les banques ont probablement les systèmes les plus perfectionnés de redondance au pays, à l'exception peut-être des sociétés pétrolières et hydro-électriques quelques cas du genre, mais dans le secteur général des affaires au Canada, je penserais que les banques ont dépensé plus d'argent pour mettre en place des mécanismes de sécurité et de redondance que toutes les autres entreprises. Et lorsqu'il s'agit de monter toute une autre installation supplémentaire d'ordinateurs, il faut de 50 millions à 100 millions de dollars pour que cela fonctionne, sans parler du personnel.

Je penserais que de nombreuses petites entreprises au pays sont bien loin d'une redondance efficace ou d'une capacité à remettre efficacement le système en marche. Elles ne peuvent peut-être pas se payer le genre de ressources nécessaires, et donc de plus en plus, on penche en faveur des ententes de réciprocité, comme l'a dit M. Jestin, en vue de chercher et de trouver dans le voisinage, du matériel et du logiciel suffisamment semblables aux siens pour pouvoir remettre le système en marche.

Lorsque de telles choses se produisent, il s'avère en général que c'est parce que le logiciel n'est pas tout à fait au point; il faut apporter des corrections afin de pouvoir fonctionner mais cela peut se faire. D'une façon générale, je suppose qu'il serait impossible d'assurer le genre de risques en jeu.

M. Beatty: Il y a probablement une différence entre les grands organismes et les petits; les grands tels que les banques, et je suppose les sociétés aériennes, pour lesquelles le réseau de réservations est essentiel, les hôtels aussi.

[Text]

Mr. MacIntosh: Yes, they would be critical.

I am not sure what the situation is in the federal government. For instance the income tax records would be a pretty critical set of files; whether they have redundancy or not I really do not know.

Mr. Beatty: Then you would tend to find it is probably in smaller institutions where you would not have proper redundancy, and often proper thought would not be given to data security either.

• 1040

Mr. MacIntosh: That is correct. In the big banks at least there is contingency planning and data security control, and it is a very sophisticated environment these days. But as you go down the size of business firm I am sure that it drops off quite rapidly.

Mr. Beatty: Thank you very much for a very helpful brief.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Thank you, Mr. Beatty.

Mr. MacIntosh, you indicated at the beginning of your remarks that in your view computer crime was quite exaggerated, and you went on at great length to explore this. Would it be fair to say that you are speaking on behalf of or with regard to banks per se and not to the rest of the corporations and the rest of the public, that it is just with regard to banks that you think it is exaggerated?

Mr. MacIntosh: Yes, that is correct, although our information obtained through the police forces would suggest that there are not very many cases in the general run of business.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Speaking to that, you also indicated that there appears to be little data . . . Of course, there is no compulsory reporting as yet; there are no specific laws with regard to "computer crime" as such; and there is also the problem of definition, in defining the word "property", for instance. So I would suggest to you that you are making an assumption that there is no computer crime based on the banking system and the sophisticated systems of control and security that you have and also based on the fact that there are inadequacies or deficiencies in the present law. Would that not be a fair statement to make?

Mr. MacIntosh: Yes, I think so.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have indicated in your statement that you feel that in some way the law should get the particulars together that refer to the software, I guess, specifically, to try and put it in some kind of a manageable form. I wonder if you could give me in a nutshell what you really mean when you say this because we are talking about either changing present laws, whether it is civil law or criminal law, or creating new ones. Could you just give us in a nutshell what you mean by this?

Ms Learmonth: Are you referring to page 1 of our brief, where we referred to organizing the computer . . .

[Translation]

M. MacIntosh: Oui, ce serait essentiel.

Je ne sais pas au juste quelle est la situation au gouvernement fédéral. Par exemple, les dossiers fiscaux seraient assez essentiels; y aurait-il redondance, je n'en sais vraiment rien.

M. Beatty: Donc cette situation aurait tendance à se manifester dans les petites organismes où on ne trouve pas la redondance nécessaire et très souvent où on n'a même pas bien réfléchi à la sécurité des données.

M. MacIntosh: C'est exact. Dans les grandes banques, du moins, il y a un plan d'urgence et un contrôle de la sécurité des données; nous vivons aujourd'hui dans un environnement très perfectionné. Mais plus les entreprises sont petites, plus le contrôle diminue rapidement.

M. Beatty: Merci beaucoup pour cet excellent exposé.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Merci, monsieur Beatty.

Monsieur McIntosh, au début vous nous avez dit qu'à votre avis on exagérait beaucoup l'importance des infractions informatiques. Vous vous êtes ensuite longuement étendu sur cette position. Devons-nous considérer que vous ne parlez que pour les banques et non pas pour les autres sociétés et pour l'ensemble du public; est-ce seulement dans le cas des banques que vous jugez cela exagéré?

M. McIntosh: Oui, absolument, mais cela dit, les informations qui nous sont communiquées par les services de police indiqueraient qu'il n'y a pas tellement de problème dans le monde des affaires en général.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À ce propos, vous dites également qu'il y aurait très peu de données . . . Evidemment, pour l'instant ces dispositions ne sont pas obligatoires, il n'y a pas de loi sur les infractions informatiques proprement dites. Il y a également un problème de définition; la définition, par exemple, du terme «biens». Par conséquent, vous prenez pour acquis qu'il n'y a pas de problème de criminalité informatique en vous fondant sur la situation dans le réseau bancaire, compte tenu du perfectionnement des systèmes de contrôle et de sécurité et également compte tenu des imperfections et des insuffisances de la loi actuelle. C'est bien cela, n'est-ce pas?

M. McIntosh: Oui, je crois que oui.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans votre déclaration vous nous dites que la loi devrait mettre les choses au point pour ce qui est du logiciel, et en particulier essayer d'en faire quelque chose d'ordonné et de compréhensible. J'aimerais bien que vous développiez rapidement cela, que vous me disiez en particulier si vous voulez changer les lois actuelles, qu'il s'agisse du droit civil ou criminel, ou bien encore si vous préférez que de nouvelles lois soient adoptées. Pouvez-vous nous dire très rapidement ce que vous voulez dire?

Mme Learmonth: Est-ce que vous pensez à la première page de notre mémoire où nous parlons de la création . . .

[Texte]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): In part on page 1, yes.

Ms Learmonth: The intention in that sentence was simply to lead into the analysis in the rest of the paper of the various types of activity that are generally referred to as computer crime, and the point was simply that if you analyse these different types of activity and recognize them for what they are and recognize the ones in which the technology is relevant and those in which the technology is really not relevant it becomes easier to establish the best legislative route. Does that answer your question?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You are looking at it, then, from a civil statute . . . not amendments to the Criminal Code?

Ms Learmonth: No, the appropriate response in any situation might be a civil statute or amendments to the Criminal Code or nothing at all and letting the common law develop. I do not think we were specifically limiting ourselves to the answer.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): In reading your brief I get the impression that you feel that the present provisions of the Criminal Code are quite adequate, although maybe somewhat limited. By the same token, we have had witnesses appear before the committee who feel that the Criminal Code provisions are totally inadequate.

One section that you referred to and which we could refer to as well is the mischief section of the Criminal Code, Section 387, where in particular we are concerned about property. At present it is my understanding that data as such is not considered as property. So there would have to be some redefining or this section would really not apply at all.

Ms Learmonth: Mr. Robinson, information is not property. I think the problem we have is this distinction between information and data. If it were deemed expedient to redefine property to include information, and if we could live with the impact of that decision on the other attributes of property at law, then the solution might be quite adequate. But if the mischief provision were altered to include data, defined as computerized data, as property, I think a problem might be created there.

• 1045

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): So you feel that the mischief section in the Criminal Code could be amended satisfactorily to include data and information, I suppose. Is that what you are saying? How broad should the word "property" be?

Ms Learmonth: I think the subcommittee has had a fair amount of evidence on that question, and the consensus seems to be, and I would agree with this, that to redefine property to include information would cause a lot of problems because of the attributes of property in other contexts in the law. It would seem to me that it might be a more direct approach to simply

[Traduction]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): C'est en partie à la première page, effectivement.

Mme Learmonth: Cette phrase sert en fait d'introduction à l'analyse que nous faisons dans le reste du document des différents types d'activités qui sont généralement désignés sous le titre de crimes informatiques; nous expliquons que si l'on analyse ces différents types d'activités, si on les situe précisément dans leur contexte, en départageant les cas où les solutions peuvent être technologiques, les cas où la technologie ne sert à rien, il devient bien plus facile de choisir une démarche législative. Cette réponse vous satisfait-elle?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous partez donc d'un statut civil et non pas d'amendements au Code criminel?

Mme Learmonth: Non, quelle que soit la situation, la solution peut passer par un statut civil, par des amendements au Code criminel ou même peut-être consister à ne rien faire du tout, à attendre que la «common law» se développe. Je n'avais pas l'impression que notre réponse était si restrictive.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): En lisant votre mémoire, j'ai l'impression que pour vous les dispositions actuelles du Code criminel sont bien suffisantes, bien que parfois quelque peu limitées. En même temps, des témoins, qui ont comparu devant nous, estiment les dispositions du Code criminel totalement insuffisantes.

Vous faites allusion à un article que nous pourrions invoquer nous-mêmes, il s'agit de l'article 387 du Code criminel sur les méfaits, en particulier touchant les biens. J'ai l'impression que pour l'instant ces données ne sont pas considérées comme des biens. Donc, si l'on tient à ce que cet article soit le moins redéfini possible, il faudrait modifier les définitions.

Mme Learmonth: Monsieur Robinson, l'information n'est pas un bien. Je pense que le problème c'est la distinction entre information et donnée. S'il était jugé utile de redéfinir la propriété pour tenir compte de l'information, à condition que nous puissions supporter les effets de cette décision sur les autres attributs en droit de la propriété, effectivement, ce serait peut-être une bonne solution. Mais si cette disposition portant sur le méfait devait être changée afin que les données enregistrées sur ordinateur soient perçues comme étant un bien, je crois qu'il pourrait y avoir un problème.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Donc, vous croyez qu'on pourrait modifier l'article du Code criminel portant sur les méfaits de façon satisfaisante afin d'y inclure les données et les renseignements, j'imagine. C'est bien ce que vous dites? Quelle portée devrait-on alors donner à la définition de «biens»?

Mme Learmonth: Je crois que le sous-comité a entendu pas mal de témoignages à ce propos et il semble que tous s'entendent pour dire, et je serais d'accord à ce propos, que redéfinir le terme de propriété pour y inclure l'information causerait beaucoup de problèmes à cause des attributs que l'on accorde à la propriété dans certains autres contextes de la loi. Il me

[Text]

treat information as something separate from property and legislate specifically on the question of information.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Are there other sections of the Criminal Code that you feel could be adequately amended for computer crime?

Ms Learmonth: I think the questions of access in use of the computer system, if those two provisions were installed in the Criminal Code it would adequately take care of the majority of specifically computer-related problems which we might identify.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Now, you indicate on page 3 of your brief that the banking system, I guess, has invested heavily in data security. I wonder if you could give us kind of an overview without giving away all the secrets of your security. How complex is it, how many steps are there that are looked at from the banking point of view? You did mention something about your back-up. I suppose that is part of your security system too, and the fact that you take records away periodically so that the whole story is not in your computer system. Could you tell us something about this data security that you have?

Mr. MacIntosh: May I ask Mr. Jestin to address that?

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Yes, fine.

Mr. Jestin: We approach the data security question or electronic data processing security question in two veins; one being an environmental set of controls, such as physical back-up, emergency power, fire detection equipment, that sort of thing, and physical premises protection, such as guards, separation of duties. We also deal with administrative and organizational control provisions, such as security policies and good business practice guidelines. We deal with telecommunication security in terms of... when appropriate, we encrypt the data transmission. Hardware security is normally available from the vendors. However, if we deem it appropriate, we apply additional safeguards. We invest in software security in terms of the operating system and the application of problem-solving software. Data security in terms of erasure of media or storage of media, we apply safeguards in that area as well.

The other dimension that we apply is in terms of the systems development approach, wherein we have a team of security specialists who participate with the systems designers in defining internal and financial control structure of an application when it is operating so that we can rely on some branch level controls in our branch network, some telecommunication

[Translation]

semble que l'on pourrait aborder la question plus directement, tout simplement en se disant que l'information est quelque chose de distinct de la propriété pour ensuite légiférer plus précisément sur la question de l'information.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Y a-t-il d'autres articles du Code criminel, d'après vous, qu'on pourrait modifier de façon adéquate afin de régler ce problème de la criminalité informatique?

Mme Learmonth: Je crois que les questions d'accès pour l'utilisation d'un système d'ordinateur, si ces deux dispositions devaient être portées au Code criminel, cela réglerait adéquatement la majorité des problèmes, plus précisément reliés à l'ordinateur, que l'on pourrait identifier.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous dites à la page 3 de votre mémoire que le système bancaire a beaucoup investi au chapitre de la sécurité des données. Je me demande si vous pourriez faire un peu le tour de la question sans pour autant nous révéler tous vos petits secrets. Quelle en est la complexité, combien d'étapes y a-t-il du point de vue des banques? Vous avez parlé d'un système de relève. J'imagine que cela fait aussi partie de votre système de sécurité tout comme le fait que vous en sortez régulièrement des dossiers de façon à ce que la masse de renseignements ne se trouve pas toute en même temps dans votre système d'ordinateur. Pourriez-vous nous toucher un mot de ce système de sécurité dont vous disposez?

M. MacIntosh: Je pourrais demander à M. Jestin de répondre à cette question?

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oui, parfait.

M. Jestin: La question de la sécurité des données ou de la sécurité du traitement électronique des données se pose en deux volets. Tout d'abord, il y a certains contrôles qui ont à voir avec le matériel, comme le matériel de réserve, groupe électrogène de secours, matériel de détection d'incendie, ce genre de choses sans oublier, évidemment, la protection des lieux et locaux par les gardiens, par la séparation des tâches et ainsi de suite. Il y a aussi l'aspect administratif et organisationnel des contrôles comme les politiques de sécurité et la conduite prudente de nos affaires. Quant à la sécurité des télécommunications, elle est assurée... Lorsque c'est approprié, nous encodons la transmission des données. La sûreté du matériel est habituellement fournie par les vendeurs. Cependant, si nous croyons que c'est approprié, nous rajoutons certains éléments nous-mêmes. Quant au logiciel, nous en assurons la sécurité en veillant au système d'opération sans oublier certains logiciels servant à résoudre certains problèmes. Pour ce qui est d'effacer les données et de stocker les bandes magnétiques, nous prenons aussi nos précautions.

Il y a aussi la dimension du développement des systèmes, c'est-à-dire que nous avons une équipe de spécialistes en sécurité qui, de concert avec les concepteurs de systèmes, définissent la structure interne et financière de contrôle d'une application lorsque le tout fonctionne, de façon que nous puissions compter sur certains contrôles au niveau des succursales de notre réseau, c'est-à-dire qu'il y a certains

[Texte]

controls, software controls, and then the traditional balancing in run-to-run type of control.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): When you use the term, and I quote right from your brief, “invested heavily in data security”, are you really talking about not only the various steps that you have to cover but the costs as well?

Mr. Jestin: Yes, sir.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Is there a substantial cost to this?

Mr. Jestin: Yes, there is. There is a substantial cost in the sense of an investment in salaries for people to review application systems to ensure their adequacy in terms of security. However, that has an immediate benefit in the reliability and accuracy of that system. So we do not view it as an overhead, we view it as a responsibility to do things right the first time.

• 1050

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I suppose the banks are in a preferred position to be able to spend whatever they need on their security, because they can charge it up to their borrowers and lenders and so on, as part of a business. I am not so sure that everybody else would be able to do the same thing, but at least you are saying that the sophistication of your security is such that if this were followed by all businesses, then there would not be a great problem as far as computer crime is concerned. I suppose you add to this the whole question of internal control mechanisms that you mentioned. You might wish to say something further on this, which might include the separation of duties that you referred to and the so-called good business practice, because I note that Mr. MacIntosh, in giving a definition of computer crime, indicated it was bad business practice.

Mr. MacIntosh: Perhaps I could say a word about some of those issues. To give you an idea of the scale of the operation in the banks. The annual operating budget would be over \$1 billion in the banking industry in Canada, to operate computer systems. There are about probably 30,000 employees in the banks, in computer systems now, out of 150,000 altogether. It is an enormous operation. Of those 30,000 employees, probably 10,000 are involved in programming and system design—a very large number of people—and with varying degrees of expertise, from junior programmers up to highly sophisticated people with PhDs in computer sciences. Because of the scale of these operations, all of the banks have computer audit and control units, such as that which Mr. Jestin supervises, and they might involve a score of people in a single institution, and their job is to test the software for internal viability, consistency and security; not just for security but also to make sure that in fact it does what you think it is supposed to do, before you put it out there as a service to the public.

[Traduction]

contrôles en matière de télécommunications, de logiciels sans oublier, évidemment, le contrôle traditionnel qui s'effectue d'un passage-machine à l'autre.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans votre mémoire, vous dites avoir «investi beaucoup pour la sécurité des données»; j'aimerais savoir si cela signifie que vous avez investi non seulement du temps mais aussi beaucoup d'argent pour faire tout ce que vous venez de décrire?

M. Jestin: Oui, monsieur.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Est-ce que cela coûte très cher?

M. Jestin: Oui. Cela coûte très cher car il faut investir en salaires pour les gens qui révisent les systèmes afin de s'assurer que les mesures de sécurité sont adéquates. Cependant, cela se traduit en gains immédiats grâce à la fiabilité et à la précision du système. Il ne s'agit donc pas de frais d'exploitation, mais plutôt de la responsabilité que nous avons de nous assurer que tout se fasse bien dès le départ.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): J'imagine que les banques se trouvent en position privilégiée lorsqu'il s'agit de dépenser ce dont elles ont besoin pour la sécurité parce qu'elles peuvent toujours en refiler les frais aux prêteurs et emprunteurs et ainsi de suite comme faisant partie des frais d'affaires. Je ne suis pas sûr que tous les autres pourraient faire la même chose, mais vous dites au moins que votre système de sécurité est tellement sophistiqué que si votre exemple devait être suivi par toutes les entreprises, il n'y aurait pas beaucoup de problèmes de criminalité informatique. J'imagine que vous ajoutez cela à tous ces mécanismes de contrôle interne dont vous avez parlé. Vous voudriez peut-être en dire plus long à ce sujet de même qu'à propos de la séparation des fonctions que vous avez mentionné et de ce que vous appelez la bonne conduite des affaires parce que je note que M. MacIntosh, en définissant le crime informatique, a dit qu'il s'agissait là d'une mauvaise conduite des affaires.

M. MacIntosh: Je pourrais peut-être vous toucher un mot de certaines de ces questions. Tout d'abord, je vais vous donner une idée de l'échelle de valeur pour les banques. Les frais de fonctionnement annuels des systèmes d'ordinateur sont de plus de un milliard de dollars dans l'industrie bancaire au Canada. Il y a peut-être quelque 30 000 employés des banques qui s'occupent de systèmes d'ordinateur, sur un total de 150 000 employés. C'est énorme. De ces 30 000 employés, probablement 10 000 sont employés à la programmation et à la conception de systèmes, c'est beaucoup de monde, et ce, à tous les niveaux, en partant des programmeurs moins spécialisés jusqu'aux gens qui ont des doctorats en informatique. À cause de l'échelle de ces opérations, toutes les banques ont des unités de vérification financière et de contrôle des ordinateurs, comme celle dont est responsable M. Jestin; on y retrouve jusqu'à une vingtaine de personnes par établissement et leur travail est de vérifier la rentabilité interne, la logique et la sécurité du logiciel. Il ne s'agit pas d'une simple question de

[Text]

Nothing is worse than to put a service out and then find it does not work. So, the testing systems that go into the preparation of something new are quite extensive.

In terms of the separation of function, for example, the software design people working on a new program. Let us say you have a new function, such as provided for in the recent budget, the ISIP, the investment planned provisions in the budget; that will involve a very extensive piece of software development by someone, perhaps by a number of people, competing people, and that would be done in a software programming unit. But those people would never have access to the place where the programs are actually operated, so they would not be in a position to go into the computer room, knowing the program and having the skill to alter the program for their own purposes. That would not happen, because you would separate—physically they are probably not even in the same building—and you would keep the functions quite separate. In fact, that is one sort of control that you have.

More generally, of course, in a bank you also have your internal audit group, who are constantly looking at the branch numbers and they are looking at the ledgers; they are looking at the hard copy. In any good business system, the computer is only as good as the ultimate audit that you can read.

Of course, I think it is fair to say that on the whole . . . —with one or two fairly unfortunate examples—the audit control systems of banks are really very strong. They are a whole lot stronger than, say, what you see when you find that the medical records in some general hospital have been thrown into the garbage can out back and they are blowing around in the wind. That, in my experience, has never occurred in the banking system in this country.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Jestin, would you carry on from there and give us some more explanation on the internal control mechanisms?

Mr. Jestin: Certainly. As you are no doubt aware, securities are balanced between the business risk and the cost of the safeguard to balance that risk. Our definition of good business practice is a prudent application of controls, so that we do not overly constrict the business we are in but we still have a high degree of integrity and reliability in the business service we are providing.

• 1055

I might just make a comment on your desire to show that small businesses may not avail themselves as easily of sophisticated data security measures. Ordinarily, when you purchase a computer system, you also purchase software; and in some cases, application systems have a set of procedures that go along with them. Today in the data processing world, software security is a tremendously important aspect; and small

[Translation]

sécurité: il faut aussi s'assurer que tout cela fait bien le travail qu'il est censé faire avant que vous ne vendiez ce service au public. Rien n'est pire que d'offrir un service pour ensuite apprendre qu'il ne fonctionne pas comme prévu. Tout nouveau système est soumis à une série de tests exhaustifs.

Pour ce qui est de la séparation des fonctions, par exemple, prenons les concepteurs de logiciel qui travaillent à un nouveau programme. Disons que vous avez une nouvelle fonction comme dans le récent budget, le RPTI, les dispositions concernant la planification des investissements; cela signifie beaucoup de travail sur un logiciel par quelqu'un, peut-être même par plusieurs personnes, des gens qui se font concurrence et cela se fera dans une unité de programmation de logiciel. Cependant, ces gens n'auront jamais accès aux lieux où on se sert des programmes et ils ne pourraient pas pénétrer dans la salle des ordinateurs, connaissant le programme et ayant toutes les aptitudes voulues pour modifier le programme à leurs propres fins. Cela ne se fera pas parce que tous ces éléments sont distincts et séparés, physiquement, ces gens ne se trouvent probablement même pas dans le même édifice, et les fonctions sont distinctes et séparées aussi. C'est là une des formes de contrôle possibles.

De façon plus générale, évidemment, dans une banque vous avez aussi votre groupe de vérification financière interne qui scrute sans cesse les affaires transigées dans chaque succursale et qui étudie les livres comptables: Ces équipes travaillent sur papier. Quel que soit le système d'affaires que vous ayez, l'ordinateur ne vaut qu'en fonction de la vérification financière finale que vous pouvez lire.

Evidemment, je crois qu'il est juste de dire, à l'exception d'un ou deux malheureux exemples, qu'en général les systèmes de contrôle et de vérification des banques sont vraiment très bons. Beaucoup mieux, disons, que ce que vous avez dans le cas des dossiers médicaux de certains hôpitaux où les dossiers ont été jetés à la poubelle et relégués dans une ruelle pour être emportés par le vent. Aucune banque de notre pays n'a jamais été mêlé à pareille histoire, à ma connaissance.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Jestin, pourriez-vous prendre la relève pour nous expliquer un peu plus en détail le fonctionnement des mécanismes de contrôle interne?

M. Jestin: Certainement. Comme vous le savez sans doute, en matière de sécurité, il s'agit d'atteindre un juste équilibre entre le risque couru et le coût impliqué pour faire diminuer ces risques. Il faut donc contrôler les choses prudemment de façon à ne pas restreindre la bonne marche des affaires, tout en nous assurant d'avoir un haut degré d'intégrité et de fiabilité dans le service que nous fournissons.

Je pourrais peut-être faire un petit commentaire sur ce désir que vous aviez de montrer que les petites entreprises ne sont pas tellement disposées à se doter de mesures de sécurité pour le traitement des données. D'habitude, quand vous achetez un système d'ordinateur, vous achetez aussi le logiciel; dans certains cas, les systèmes d'application s'accompagnent de procédures. Aujourd'hui, dans le monde du traitement des

[Texte]

businesses can avail themselves of hardware and software which has intrinsic within it sophisticated safeguards, so they are not at sea with the world of computing. They have some assistance upon which they can draw.

In terms of good business practice and the separation of duties, I guess the best example to show is that daily we operate business services nationwide. Those systems are called production systems. We separate the people who are responsible for production systems and those who are responsible for developing new systems. The computing resource which is associated with each of those entities is separated, and those boundaries are not compromised.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Getting down to the nitty-gritty of this, do you have special courses or special periods of training for the employees who are involved in data processing and in computer work and programming, with regard to security?

Mr. Jestin: I cannot speak on that issue, specifically. I can speak on it specifically to the bank I represent. In terms of the Canadian Bankers' Association, I am not familiar with their security awareness.

The bank I represent is, in fact, participating in a security awareness program which does present the responsibilities, the ethical requirements and the confidentiality aspects to employees.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Maybe Mr. MacIntosh could tell us more. He has indicated that there is a sophisticated set-up of controls and I suppose telecommunications and what not. But are the people themselves actually alerted to this? Are they aware of the so-called computer crime? Are they trained or instructed in how to control the data processing equipment, how to control the computers, their responsibility with regard to programming and so on?

Mr. MacIntosh: Yes, I think I could perhaps add a little bit. It happens that I was once responsible for the computer system operations of the same bank from which Mr. Jestin comes, so I cannot speak about other individual banks. But speaking generally for the association, there is a tremendous volume of educational expenditure on computer systems skills of all kinds, including, of course, security skills.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You have indicated in your statement that, in your view, the problems of computer abuse will not be solved merely through legislation, and you have indicated two approaches. One is the internal controls, and the other is professional ethics. You talked to some extent about the internal controls, but do you have a code of ethics for the

[Traduction]

données, la sécurité du logiciel joue un rôle très important; les petites entreprises peuvent se trouver du matériel et du logiciel dont la sécurité est intrinsèque et elles ne sont donc pas sans moyen de défense dans le monde hostile de l'ordinateur. Elles peuvent faire appel à toutes sortes de ressources.

Pour ce qui est de la bonne conduite des affaires et la séparation des fonctions, je crois que le meilleur exemple à vous donner est de vous dire que, quotidiennement, nous fournissons des services à l'entreprise à l'échelle de la nation. Ces systèmes sont dits système de production. Nous séparons les gens responsables des systèmes de production de ceux responsables du développement de nouveaux systèmes. Les ressources informatiques mises à la disposition de chacun de ces deux groupes sont distinctes et séparées et l'on veille à ce que les frontières ne soient pas franchies.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Pour en venir à la substantifique moelle de toute cette question, avez-vous des cours spéciaux ou des périodes spéciales de formation pour ces employés qui s'occupent de traitement des données, d'ordinateurs et de programmation, surtout pour ce qui a trait à la sécurité?

M. Jestin: Je ne puis répondre de façon précise à cette question. Je peux vous donner certaines précisions sur ce qui se fait à la banque que je représente. Pour ce qui est de l'Association elle-même, je ne suis pas au courant de tous les détails.

La banque que je représente participe à un programme de sensibilisation à la sécurité qui explique aux employés les divers aspects de responsabilité, d'éthique et de discrétion.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Peut-être M. MacIntosh pourrait-il nous en dire plus. Il nous a laissé comprendre qu'il y a tout un réseau complexe de contrôles et, j'imagine, de télécommunications et le reste. Mais les gens sont-ils vraiment bien renseignés à ce propos? Sont-ils au courant de ces fameux crimes utilisant les ordinateurs? Leur a-t-on donné une certaine formation ou les a-t-on renseignés sur la façon de contrôler le matériel de traitement des données et les ordinateurs ainsi que sur leurs responsabilités concernant la programmation et le reste?

M. MacIntosh: Oui, je crois que je pourrais vous donner des précisions supplémentaires. Justement, j'étais jadis responsable des opérations du système d'ordinateur de la même banque dont vient M. Jestin et je ne puis donc rien dire des autres banques. Cependant, de façon générale et parlant au nom de l'Association, on dépense énormément d'argent pour la formation et l'instruction afin d'améliorer la compétence des employés à tous les niveaux, y compris, évidemment, au niveau des mesures de sécurité.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Dans votre déclaration, vous dites que, d'après vous, les problèmes d'abus des ordinateurs ne se résoudront pas tout simplement grâce à une loi et vous donnez deux façons d'aborder la question. Tout d'abord, le contrôle interne et, ensuite, l'éthique professionnelle. Vous avez donné certains détails sur les contrôles internes, mais avez-vous un code d'éthique professionnelle pour les programmeurs et les gens qui

[Text]

programmers and people involved in computer data processing?

Mr. Jestin: We have a code of ethics relative to business practice bank-wide. We do not specialize the responsibilities strictly to the data processors, because all aspects of the banking industry are somehow touched by computing. Many of the tenets of those guidelines are items such as confidentiality of customer data being of paramount importance, not compromising yourself in terms of business responsibility.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): You indicate that the internal controls and the professional ethics should go a long way to moderating the concerns you have about computer security. What other suggestion would you make that could be carried out either through the users directly or by the law to ameliorate your concerns even further?

• 1100

Mr. Jestin: I do not have any, personally, in addition to the ones presented in the brief. I participated in the task force and they represent my beliefs.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): We are having a lot of interference with the bells. I am pretty well finished with my questioning anyway. There are a couple more I would like to ask. I would turn to page 11 of your brief, if you have it there, where you indicate toward the end of the page that there are three things; you say:

Certainly, the criminal law may be an appropriate vehicle with which to deal with some situations, although to date the Criminal Code in Canada has not prohibited the theft, copying or other abuse of information. The definition of new crimes may be required or, in some cases, existing sections of the Criminal Code may be slightly amended to accommodate new technology. However, privacy legislation, trade secrets law and copyright also regulate the treatment of information in this country . . .

I wondered if you wanted to explain further the latter part on privacy legislation and other laws we presently have on the books, such as trade secrets law and copyright law. I wanted to ask you if you want to indicate your objection to mandatory reporting.

Ms Learmonth: I do not think we have any specific comments to expand on that paragraph. It has been mentioned already during this session that the Copyright Act might be an appropriate vehicle for dealing with copying of software. Clearly, questions of privacy may arise if confidential information is stored in a computerized or non-computerized environment. This was all the reference to privacy legislation was intended to refer to.

The reference to trade secrets law was a reference to the fact that some of these questions may not require legislation at all.

[Translation]

oeuvrent dans le domaine du traitement des données par ordinateur?

M. Jestin: Nous avons un code d'éthique professionnelle général que l'on doit observer. Nous n'avons pas de code spécialisé pour ce qui est des responsabilités strictes concernant le traitement des données parce que l'industrie bancaire est tout simplement envahie de toutes parts par l'ordinateur à l'heure actuelle. Ce code d'éthique insiste surtout sur des choses comme l'importance de la discrétion absolue à l'égard des données des clients ou encore sur comment faire pour respecter ses responsabilités face au monde des affaires.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Vous dites que les contrôles internes et que le code d'éthique professionnelle vous rassurent énormément lorsque vous songez aux problèmes reliés à la sécurité dans le domaine des ordinateurs. D'après vous, que pourrait-on faire de plus pour augmenter encore votre assurance face à toute cette question?

M. Jestin: Personnellement, je ne vois pas ce qu'on pourrait rajouter à part ce que nous avons déjà présenté dans le mémoire. J'ai fait partie du groupe d'étude et je souscris à ce qui a été dit.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Les cloches sont un peu gênantes. De toute façon, j'avais presque fini de poser mes questions. Il y a une ou deux autres questions, cependant, que j'aimerais poser. Je vous reporte à la page 11 de votre mémoire, si vous l'avez à portée de main, où vous dites vers la fin de la page qu'il y a trois choses; vous dites:

Il n'y a pas de doute que le droit criminel constitue un véhicule approprié dans certains cas, bien que le Code criminel du Canada n'interdise pas encore le vol et la reproduction d'information ni les autres infractions s'y rattachant. Il faudra peut-être arriver à définir les nouveaux crimes ou, dans certains cas, amender certains articles du code à la lumière de la nouvelle technologie. Toutefois, la loi sur la protection des renseignements, celle sur les secrets commerciaux et la loi sur le droit d'auteur contiennent des dispositions s'appliquant à l'information . . .

Je me demandais si vous vouliez nous donner davantage d'explications sur ces lois qui existent déjà. Je voulais vous demander si vous vouliez nous faire savoir que vous vous opposez à la dénonciation obligatoire.

Mme Learmonth: Je ne crois pas que nous ayons de commentaires précis à faire à propos de ce paragraphe. On a déjà dit aujourd'hui que la Loi sur les droits d'auteur pourrait peut-être servir pour la copie de logiciels. Il est clair que les questions de protection peuvent se poser si des renseignements confidentiels sont emmagasinés dans un ordinateur ou ailleurs. C'est tout ce que signifie cette référence à la loi protégeant la vie privée.

Quant à la loi sur les secrets commerciaux, il s'agit tout simplement de préciser que certaines de ces questions n'ont

[Texte]

Common law may be sufficient to deal with problems which are essentially civil matters and which can be settled between two parties. I am afraid I cannot elaborate any further on that. We would want to view all of these questions as a whole in the context of an investigation into information policy and comprehensive information legislation or study.

Mr. MacIntosh: If I could add a word, Mr. Chairman, about the issue of mandatory reporting of computer-related crimes, we just think that this is over-kill. The only mandatory reporting of a crime in Canada, I believe, is treason or high treason. It seems to me a computer offence is a whole long way from that. There is no such thing as mandatory reporting of a break-in of your house. I do not think people always report a break-in of their house to the police. They may consider that it is not worth the trouble, I suppose. But I do not think we have mandatory reporting of any other crimes in this country. We do not feel there is any reason to single out this area for mandatory reporting any more than there would be for any other crime.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): I do not agree with you that there is no mandatory reporting in the Criminal Code. There certainly is. You just go out driving in Ottawa here and get into an accident and leave the scene of the accident. You will soon find there is a requirement under the Highway Traffic Act and also under the Criminal Code that you should have reported it or you could be in serious trouble. But that is beside the point.

I think I will leave it at that, except for one question. You indicated someplace in your statement that you felt there should be a further study done. I just do not recall what part of your statement it was in . . .

• 1105

Ms Learmonth: Perhaps on page 11—the first section of paragraph 14.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Oh, yes:

The question of how to deal with information as a whole requires further study.

What are you really suggesting as part of that further study? Are you talking of definition?

Ms Learmonth: No. This comment arose primarily out of our concern with the Department of Justice's proposed problems and solutions. Those included references to the alteration and destruction of data. Our concern was primarily that those types of activity relating to information not be separated from the acquisition, use, and disclosure of information.

[Traduction]

peut-être pas à faire l'objet d'une loi spéciale. Il se pourrait que la common law suffisse lorsqu'il s'agit de traiter de problèmes relevant essentiellement des tribunaux civils et qui peuvent être réglés entre deux parties. Je suis désolée de ne pouvoir en dire davantage à ce propos. Toutes ces questions font partie d'un tout dans le contexte d'une enquête sur les politiques d'information ou d'une étude globale sur la législation de l'information.

M. MacIntosh: Si vous me permettez d'ajouter un mot, monsieur le président, concernant la dénonciation obligatoire lorsqu'il y a un crime informatique, nous croyons que c'est tout simplement aller trop loin. Je crois que le seul crime, au Canada, pour lequel on exige une dénonciation obligatoire, c'est la trahison ou la haute trahison. Il me semble qu'un crime relatif aux ordinateurs ne se classe surtout pas dans une de ces catégories. Rien ni personne ne vous oblige de rapporter à la police qu'il y a eu entrée par effraction dans votre domicile. Je ne crois pas que les gens appellent toujours la police lorsque c'est le cas. Peut-être trouvent-ils que cela n'en vaut pas la peine. Mais je ne crois pas que la loi impose la dénonciation obligatoire pour d'autres genres de crimes au Canada. Nous ne comprenons pourquoi il devrait y avoir dénonciation obligatoire pour ce genre de crimes tandis qu'il n'y a pas de telles exigences dans le cas d'autres crimes.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Je ne suis pas d'accord pour dire que la dénonciation obligatoire ne se retrouve nulle part ailleurs au Code criminel. Au contraire. Sortez d'ici pour vous promener en automobile dans la ville d'Ottawa et trouvez-vous impliqué dans un accident de voiture: quittez ensuite les lieux de l'accident. Vous apprendrez très vite qu'en vertu du Code de la route et du Code criminel vous devez rapporter l'accident sinon vous vous trouverez dans de sérieuses difficultés. Mais tout cela n'a rien à voir.

Je crois que je m'en tiendrai là sauf pour une dernière question. Quelque part dans votre déclaration, vous avez dit qu'il vous semblait qu'on devrait étudier davantage la question. Je ne me souviens pas au juste où cela se trouvait . . .

Mme Learmonth: Peut-être à la page 11 . . . la première partie du paragraphe 14.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Oh, oui:

Aborder la question de l'information dans son ensemble exige, de toute évidence, une étude préalable poussée.

Que voulez-vous dire par là? S'agit-il de définitions?

Mme Learmonth: Non. C'est tout d'abord parce que nous étions préoccupés des problèmes et solutions proposés par le ministère de la Justice. On y parlait de modification et de destruction de données. Nous ne voulions tout simplement pas que ces deux éléments soient traités distinctement de l'acquisition, de l'utilisation et de la divulgation de l'information.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Mr. Beatty, do you have a question?

Mr. Beatty: I have one last question that I cannot resist asking. You seem quite confident in the security systems advanced; I remember when I was in Treasury Board that the officials there were very confident in the security systems in the government. Have any of your members contracted with any experts in computer security and given them the responsibility of testing their computer systems by attempting to gain unauthorized access to them? It seems to me that would be the best test of the security. We have had experts testifying before the committee who have said—and I am inclined to agree with them—that no system is unbeatable, whether physical or electronic, that perhaps the best way of testing any the quality of security in any system is take an expert and to put him on contract and to invite him to attempt to break in.

Mr. Jestin: Well again, I would preface my remark by saying that security is a balance between the cost of the safeguard, and the business risk. You are absolutely correct; there is no secure vault or computer system from attempted attack that has no cost boundaries. In the security institute, we refer to that as a work factor, and we try to balance the work factor to the business risk. In terms of your question about whether or not we engage consultants in attempting to break down our computer systems or to penetrate them, the answer is yes and no. Yes, we engage consultants to independently review the adequacy of our security provisions. However, to my knowledge we do not engage them in a “tiger-team” approach, to which the U.S. military referred, in an attempt to penetrate our systems.

Mr. Beatty: The University of Waterloo, for example, does encourage students to attempt to test the security of their system, as a means of giving them the information they need to upgrade security.

But one of the things we are dealing with, I think, in computer systems, unlike physical attacks on banks, is that we are dealing with a very different set of ethics, where it is deemed to be a bit of a lark, sport, to attempt to break into a computerized system. I mean, just for the sake of having done it, not to defraud or to steal or to take any particular benefit other than the thrill of success. It seems to me that potential violators of computerized systems are a different clientele from the potential thieves who would break into a bank in other ways, and that it might be useful to have something similar to a tiger team or something similar to the system they have at the University of Waterloo, whereby you could actually encourage a test to be made of your system to give yourselves the assurance that it is secure.

Mr. Jestin: My comments were of specifically external people. Internally, we have a philosophy called “user acceptance testing”, which attempts to fully test out a system before it is introduced into production. During that type of hurricane simulation, if you will, we try to utilize out-of-reach conditions and exceptional conditions, in order to fully exercise the

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Monsieur Beatty, vous voulez poser une question?

M. Beatty: Une dernière question à laquelle je ne puis absolument pas résister. Vous semblez avoir toute confiance dans les mesures de sécurité proposées. Je me rappelle que lorsque j'étais au Conseil du Trésor, les fonctionnaires de cet organisme avaient toute confiance au système de sécurité du gouvernement. Est-ce que d'aucuns de vos membres auraient accordé des contrats à des experts en sécurité dans le domaine de l'informatique pour leur donner mandat de mettre à l'épreuve leur système en essayant d'y accéder sans en avoir l'autorisation voulue? Il me semble que ce serait là la meilleure épreuve à laquelle on puisse les soumettre. Il y a bien des témoins experts qui ont dit au Comité, et j'ai tendance à les croire, qu'il n'y a pas de système parfait, qu'il s'agisse du matériel ou du logiciel, et que peut-être la meilleure façon de vérifier le degré de sécurité d'un système est de passer un contrat avec un expert pour l'inviter à jouer au criminel.

M. Jestin: Encore une fois, je tiens à dire tout d'abord qu'en matière de sécurité, il faut chercher le juste milieu entre le facteur sécurité et le facteur risque. Vous avez tout à fait raison: il n'y a aucune chambre forte ni aucun ordinateur qui soit absolument à l'abri de tout si l'on tient compte des coûts. En terme de sécurité, cela s'appelle le facteur travail et nous cherchons à atteindre un juste milieu entre le facteur travail et le risque. Quant à savoir si nous engageons des experts pour essayer de pénétrer nos systèmes ou d'y avoir accès illégalement, la réponse est oui et non à la fois. Oui, nous payons des experts indépendants pour étudier nos dispositions sécuritaires. Cependant, à ma connaissance, nous n'employons pas une «équipe de baroudeurs» dont parlaient les militaires américains, pour essayer de pénétrer nos systèmes.

M. Beatty: L'Université de Waterloo, par exemple, encourage ses étudiants à essayer de déjouer les mesures de sécurité de son système ce qui permet évidemment à cette institution de déceler les failles et d'y remédier.

Enfin, lorsqu'il s'agit d'ordinateur, je crois qu'il y a le problème suivant: contrairement à ce qui se passe pour les vols à main armée, les gens semblent croire que «ça fait sportif» de s'attaquer à un ordinateur. Du moins, s'y attaquer tout simplement pour avoir la satisfaction de réussir le coup, pas pour perpétrer une fraude ou voler quoi que ce soit ni en tirer un avantage particulier. Il me semble que les gens qui font ce genre de choses sont différents de ces voleurs qui s'attaqueraient à une banque de diverses autres façons et il serait peut-être utile de mettre sur pied une «équipe de baroudeurs» ou d'adopter une méthode semblable à celle préconisée par l'Université de Waterloo et vous pourriez encourager certaines personnes à mettre à l'épreuve votre système tout simplement pour vous assurer que tout va bien.

M. Jestin: Je parlais précisément de gens de l'extérieur. En nous servant de nos ressources internes, nous appliquons notre philosophie de «test pré-utilisation» grâce auquel on met à l'épreuve un système avant qu'il ne serve en réalité. Pendant ces épreuves qui tiennent de la guerre éclair, si vous voulez, nous imaginons des conditions inimaginables et exceptionnelles

[Texte]

software. Of course, that is never perfect. However, it does increase the reliability of the systems tremendously. Personally, I do not ascribe to having our own employees purposely attempting to penetrate the system, because I do not believe that is focusing their jobs . . .

• 1110

Mr. Beatty: Energies in a constructive way.

Mr. Jestin: Well, their responsibility to the organization is certainly to secure it, but it is not to attempt to joyride on the organization; I believe that it is less ethical to do that than to have an approved user acceptance type of forum with which to exercise that type of zeal.

Mr. Beatty: The University of Waterloo used to offer students a jug of beer if they could crack the system. You are not thinking of something similar for the banks?

Mr. Jestin: No.

Mr. MacIntosh: It would have to be cider.

Mr. Beatty: Cider. Thank you very much, Mr. MacIntosh.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): One further question: With regard to this so-called mandatory reporting that may or may not be put forth, would it be your view that because of the sophistication of your own security this is not really necessary, that it is going to happen so infrequently it could be considered an internal matter only and not of concern to the public generally? Would you also agree that if there are others using computer processing or using data processing and so on, that do not have the same kind of security, that maybe this would be important, requiring them to sort of smarten up and take care of the information they have and the equipment they have in this area?

Mr. MacIntosh: Mr. Chairman, my feeling is that it would be an excessive invasion of the state into private activity to have a mandatory reporting of crime, and that it would provide a precedent that could be applied to any number of crimes in the country. If you have mandatory reporting, it is going to turn the country into a nation of snoops.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): From your knowledge, do you know if the banking system in Canada or banks generally have had any losses they can contribute to so-called "computer crime"?

Mr. MacIntosh: No, sir. We have no cases at all, no evidence other than the very marginal one I mentioned at the beginning of loss of funds on computer crime. We get a lot more evidence of out-and-out theft, burglary, and so forth.

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Could that be related to the fact that you do have such a sophisticated system of security?

Mr. Jestin: We certainly believe so. Our byword is prevention, rather than detection after the event.

[Traduction]

pour faire passer un mauvais quart d'heure au logiciel. Evidemment, ce n'est jamais parfait. Cependant, cela augmente énormément la fiabilité des systèmes. Personnellement, je ne crois pas en ce genre de procédé, c'est-à-dire encourager nos employés à essayer de déjouer le système parce que je ne crois pas que ce soit là employer leur . . .

M. Beatty: . . . énergie de façon constructive.

M. Jestin: Enfin, leur responsabilité vis-à-vis de l'entreprise, c'est évidemment d'assurer la sécurité du système, mais pas de s'amuser au frais de la princesse. Je crois que c'est moralement moins bon de faire cela que de procéder comme nous le faisons.

M. Beatty: L'Université de Waterloo offrait de payer un pot de bière aux étudiants s'ils réussissaient à pénétrer le système. Les banques ne songent pas à offrir une récompense semblable?

M. Jestin: Non.

M. MacIntosh: Il faudrait que ce soit du cidre.

M. Beatty: Du cidre. Merci beaucoup, monsieur MacIntosh.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Une dernière question. Pour ce qui est de cette dénonciation obligatoire qui sera peut-être imposée ou peut-être pas, croyez-vous que ce n'est vraiment pas nécessaire à cause de la complexité de vos propres systèmes de sécurité et qu'il y aurait si peu d'infractions que cela n'intéresserait que la banque et non pas le grand public? Ne diriez-vous pas aussi que Si d'autres se servent de traitement des données par ordinateur ou en font sans avoir le même genre de mesures de sécurité que les banques, que ce pourrait alors être important et que cela les obligerait, en quelque sorte, à se retrousser les manches pour veiller à la sécurité des données et du matériel qu'ils ont dans ce domaine?

M. MacIntosh: Monsieur le président, ce serait une invasion excessive de la vie privée par l'état s'il y avait dénonciation obligatoire d'un crime et cela constituerait un précédent qui pourrait alors s'appliquer à toutes sortes d'autres crimes au pays. S'il y a dénonciation obligatoire, vous allez faire de nous une nation de délateurs.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): À votre connaissance, pour ce qui est du système bancaire canadien ou des banques en général, savez-vous s'il y a eu des pertes attribuables à la «truandique»?

M. MacIntosh: Non, monsieur. Aucun cas du tout, rien sauf le cas marginal dont j'ai parlé au début, soit des pertes de fonds dues aux crimes commis par ordinateur ou à la truandique, comme vous dites. Il y a beaucoup de vols avérés, de vols par effraction et ainsi de suite.

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Est-ce que ce serait parce que votre système de sécurité est si complexe?

M. Jestin: Nous le croyons certainement. Nous préférons prévenir plutôt que guérir.

[Text]

The Acting Chairman (Mr. Robinson (Etobicoke—Lakeshore)): Well, thank you very much for appearing; that is, the witnesses from the Canadian Bankers' Association. It has been another point of view, and we are very glad to have had you appear before us.

The next subcommittee meeting will be on Tuesday, May 31, 1983 at 3.00 p.m. in this same room, 208 West Block, with representatives from the Canadian Consumers' Association.

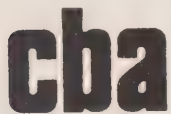
The meeting is adjourned.

[Translation]

Le président suppléant (M. Robinson (Etobicoke—Lakeshore)): Bon, alors merci beaucoup pour votre présence ici. Nous remercions les témoins de l'Association des banquiers canadiens. Nous avons entendu un autre son de cloche et nous sommes heureux de vous avoir eu parmi nous.

La prochaine réunion du sous-comité se tiendra le mardi 31 mai 1983, à 15h00, dans la même salle, 208, Edifice de l'ouest et nous entendrons des représentants de l'Association des consommateurs du Canada.

La séance est levée.



APPENDIX "COMP-2"

The Canadian Bankers' Association

BILL S-33

THE CANADA EVIDENCE ACT, 1982

A SUBMISSION TO THE

SENATE COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

MAY 1983

THE CANADA EVIDENCE ACTI. Introduction

Bill S-33 offers a unique opportunity to revise Canadian evidence law. As our contribution to this revision process, we wish to raise with the Senate Committee on Legal and Constitutional Affairs our concerns about several provisions of Bill S-33 relating to business records. It is our view that some major problems in current evidence law relating to computer-produced records are not addressed in the business records provisions of Bill S-33. As a result, we fear that Bill S-33, if enacted, will perpetuate existing uncertainty about the evidentiary status of computer-produced records. The opportunity to clarify the law in this area will have been lost.

II. The Problem of Foundation Evidence

For decades, special evidentiary rules have applied to the records of financial institutions. These rules developed because courts found that the records of financial institutions were highly reliable. In view of the accuracy of these records, it was determined that the staff of financial institutions need not be required to personally attend during court proceedings to prove the record.

An example of special legislation for this purpose is the Bankers' Books Evidence Act passed in the United Kingdom in 1879. A corresponding provision in Canadian law, first enacted in 1927, is currently set out in section 29 of the Canada Evidence Act. Section 29 provides that copies of bank records are admissible as prima facie proof of their contents. An affidavit signed by a bank manager attesting that (1) the book or record was, at the time of the making of the entry, one of the ordinary books or records of the financial institution, (2) the entry was made in the usual and ordinary course of business, (3) the book or record is in the custody or control of the financial institution, and (4) the copy is a true copy thereof, is sufficient to prove the record for the purpose of its admission as evidence.

In the years since section 29 was first enacted, the nature of bank records has changed considerably. In order to accommodate staggering volumes of daily transactions that exceed five million items each day, Canadian financial institutions have moved from manual to automated record-keeping and from long-term document storage to microfilm and microfile archive files. The computer is central to today's record-keeping system. Today, the vast majority of financial transactions are performed by automated means.

While section 29 of the Canada Evidence Act is well-suited to manually-produced records, difficulties arise when one seeks to apply section 29 to computer-produced records. The most important case illustrating this difficulty is the Ontario Court of Appeal decision in R v. McMullen.¹

The McMullen case determined that a computer printout of entries stored in a bank's computer fell within the scope of section 29. In effect, the court decided that a printout was a copy of the record contained in the computer. The court then went on to state that evidence about the

¹ R. v. McMullen (1978) 100 D.L.R. (3d) 671

reliability of the computer system would be required in order to satisfy the court that the printout was a "true copy" of the record contained in the computer system. In the words of Mr. Justice Morden of the Ontario Court of Appeal:

"I accept that the demonstration of reliability of computer evidence is a more complex process than proving the reliability of written records. I further accept that as a matter of principle a Court should carefully scrutinize the foundation put before it to support a finding of reliability, as a condition of admissibility ... The four conditions precedent provided for in (section 29)... have to be proven to the satisfaction of the trial Judge. The nature and quality of the evidence put before the Court has to reflect the facts of the complete record keeping process - in the case of computer records, the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation....If such evidence be beyond the ken of the manager, accountant or the officer responsible for the records... then a failure to comply with section 29(2) must result and the print-out evidence would be inadmissible."
(p.679)

An example of further consideration by the courts to the issue of the admissibility of computer-produced records is the more recent Ontario Court of Appeal decision in R v. Bell and Bruce.² The court in this case determined that the printout in question was an original, not a copy, because the inputted contents of the record had been intentionally erased in the computer system. Since the printout was considered an original, foundation evidence was not required to prove the reliability of the computer system.

Despite the Bell and Bruce judgment, the McMullen, decision continues as case law authority supporting the need for foundation evidence. It is, consequently, not clear to what extent foundation evidence about computer systems is required in order to establish a basis for admitting computer printouts as evidence in court proceedings. In our view, this question remains unresolved if Bill S-33 is enacted because section 130(c) of the Bill gives legislative force to the approach set out in the McMullen decision.

Section 130(c) of the Bill S-33 states that an "original" record means, in part,

² R v. Bell and Bruce (1982) 35 O.R. (2d) 164

(c) in relation to stored or processed data or information, any printout or intelligible output that reflects accurately the data or information or is the product of a system that does so.; (emphasis added)

Section 130(c) appears to express the intent that, in order to obtain the admission of a printout, it will be necessary to satisfy the court that the printout accurately reflects the data or information entered into the system. In order to demonstrate that a printout meets the requirements of section 130(c), it will be necessary for evidence to be given, orally or by affidavit, by bank employees attesting to the reliability of the system. The Bill fails to set out any detailed criteria as to the admissibility of computer printouts. Bill S-33 leaves the detailed criteria for authentication open for determination by the courts. Since the courts will have regard to the McMullen decision in developing these criteria, the lack of criteria in the Bill could result in the need for voluminous foundation evidence to prove the reliability of a computer system.

III. Reasons for Concern

The Canadian Bankers' Association has two principal concerns arising from the proposed section 130(c) of Bill S-33. First, the lack of direction to the courts with respect to foundation evidence about bank computer systems poses a potential danger to the security of those systems and customer data. Secondly, Bill S-33 is not clear about whether evidence to support the admissibility of computer-produced records can be presented by way of an affidavit prepared by a bank employee. As a result, more occasions may arise where bank personnel are required to give oral testimony in proceedings in which their banks are not involved. The inconvenience caused thereby would be inconsistent with the legislative purpose underlying section 29 of the Canada Evidence Act and return the banks to a position similar to that which existed prior to 1879.

IV. The Threat to Security

In our view, unless there is an express statutory provision protecting the secrecy of computer procedures, the possibility clearly exists that a court will be persuaded that certain information is relevant and therefore

compellable notwithstanding that disclosure of the information might be prejudicial to the security interests of the financial institution. For example, a court may seek answers to questions regarding methods of obtaining access to computer systems, the number of employees that can input into the system and receive information from it, the types of security checks performed to assure that employees will not misuse the information, and a host of other questions dealing with the potential for error and dishonesty affecting the computer system. If much of this information becomes a matter of public knowledge, efforts by financial institutions to maintain a high level of system security could be jeopardized.

Customers rely on financial institutions to maintain secure systems. The courts themselves have recognized that financial institutions are under a common law duty of confidentiality respecting customer data.³ This duty recognizes the fact that customers provide financial institutions with a large amount of sensitive information about themselves. In order to protect customer data and prevent unauthorized access to a financial institution's

³ Tournier v. National Provincial and Union Bank of England
(1924) 1 K.B. 461

computer system, it is necessary that all elements of the system be kept absolutely confidential. In order to enhance the level of safeguards, many financial institutions separate their computer systems into subsystems. Some of these subsystems are designed to test the security of the system while others actually provide the security. In many instances, it will not be possible to reveal in detail how printouts or intelligible output from computer equipment are produced without also revealing something about the procedures designed to provide security for the system.

There are no provisions of Bill S-33 setting limits to the kind of disclosure that a financial institution must make about its computer system. The possibility clearly exists that in some circumstances harmful disclosure might be required of a financial institution.

V. The Convenience Factor

Viewed in isolation, section 157 of Bill S-33 seems to give the records of financial institutions evidentiary status similar to that contained in section 29 of the Canada Evidence Act while section 155(2) appears to provide for the

use of affidavit evidence to prove a business record for the purpose of admission. Nevertheless, we are concerned that the courts might not regard affidavit evidence as a sufficient means of providing foundation evidence about a computer system. This concern arises from the apparent inconsistency that exists between sections 157 and 155(2) of the Bill on the one hand and section 130(c) on the other. It is not clear that affidavit evidence is acceptable to prove that a printout "reflects accurately" the data or information entered into the system. If affidavit evidence is not acceptable, oral testimony would be required to obtain admission of a computer produced record and the apparent underlying purpose of sections 157 and 155(2) of the Bill would be defeated.

Whereas it would have been inconvenient for bank personnel to give oral testimony concerning manually produced records, the inconvenience is compounded in the case of computer-produced records. For instance, many record-keeping systems cannot be attested to in their entirety by any one witness. The fact that no one person knows the whole system is an important security precaution. In order to prove the reliability of the whole system, therefore, more than one bank employee would be required to attend at court to give evidence. Also, the personnel who understand the system and

who, therefore, are likely to be called to give evidence, are not local branch personnel but rather staff members from regional data centres or head office systems departments who cannot be spared from their operational duties for long periods of time without serious cost and inconvenience.

We suggest that Bill S-33 should recognize the essential reliability of bank computer systems by facilitating the use of the affidavit procedure in relation to bank computer records. The reliability of these systems is evidenced by the vast volumes of transactions that pass through the banks' computer systems each day. If there is a defect in the system, this will soon be detected or come to light. The absence of any indication of a problem in the system at or about the time of the alleged offence should be sufficient proof to meet the standard of reliability established by section 130 (c).

For this reason, in our view, Bill S-33 should be drafted so that it is clear that the affidavit procedure for proving business records is available in the case of computer-produced records of financial institutions. In

addition, the Bill should set out specific criteria, the satisfaction of which would be sufficient to support the admissibility of computer-produced records by affidavit. These criteria should be such that it will be possible for a financial institution to meet the criteria in an affidavit by a branch officer without disclosing sensitive information about the institution's systems. If the Bill is amended in this manner, we feel that the underlying purpose of section 29 of the existing Canada Evidence Act and sections 157 and 155 (2) of the proposed Act will be preserved while, at the same time, removing some of the current uncertainty pertaining to the admissibility and proof of computer-produced records.

Examples of Criteria

It is remarkable to us that, although electronic data-processing is a central feature of modern record-keeping, Bill S-33 pays scant attention to these developments. Other jurisdictions have legislated specific criteria governing the admissibility of computer-produced records. Consequently, the changes we recommend to Bill S-33

are not without precedent. For instance, the report of the Federal/Provincial Task Force on the Uniform Rules of Evidence, upon which Bill S-33 is purportedly based, suggested three criteria for the admissibility of computer evidence:

1. proof that the data upon which the computer record is based is of a type regularly supplied to the computer during the regular activities of the organization from which the record comes;
2. proof that the entries into the data base from which the record originates were made in the regular course of business; and
3. proof that the computer program used in producing the record reliably and accurately processes the data in the data base.

While the third criterion could conceivably result in the release of sensitive information about a bank's computer programs, the Task Force states in its report that it should be possible to satisfy this test by providing evidence of

business experience with the computer program over a period of time. In addition, the Task Force unanimously recommends that the criteria of admissibility be capable of proof by an authenticating affidavit based on the knowledge and belief of the affiant.

Another example of criteria for admissibility of computer-produced records is contained in section 5(2) of the Civil Evidence Act of the United Kingdom enacted in 1968. This provision sets out the following criteria of admissibility for computer printouts in court proceedings:

1. proof that the printout resulted from regular use of the computer for activities carried on;
2. proof that the computer was regularly supplied with information of the kind produced;
3. proof that the computer was operating properly, or that defective operation did not affect the accuracy of the computer, and,
4. proof that the information was derived from that supplied to the computer in the ordinary course of activities.

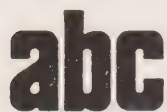
The inclusion in Bill S-33 of criteria of the sort suggested by the Task Force or set out in the U.K. Civil Evidence Act together with a provision clearly authorizing the submission of such evidence by affidavit would greatly improve the business records provisions of the Bill while not diminishing the rights of a party litigant before the courts.

Conclusion

Bill S-33 is the result of much time and effort and we expect that it will constitute the foundation of Canadian evidence law for many years to come. It is with some disappointment, therefore, that we note that areas of uncertainty under the existing Act remain unresolved. Our concern about the lack of criteria governing the admissibility of computer-produced records and our uncertainty about the use of the affidavit procedure does not exhaust the questions we have arising from Bill S-33. We are uncertain, for instance, about the status of a document produced by a system where a paper original has been destroyed, such as might occur with cheque truncation. Is the document an "original" within the meaning of section

130 (c) or is it a "copy" of an original to be dealt with according to section 133 (a) of Bill S-33? We note that the term "copy" in Bill S-33 is not defined despite the uncertainty associated with this word following the McMullen and Bell and Bruce decisions to which we have referred. In view of the frequency with which information in original documents is reproduced in different media while the original documentation is destroyed, as authorized in the case of banks by sections 157 and 159 of the Bank Act, we can only expect that further litigation will arise from a failure in Bill S-33 to take proper account of these aspects of the automated record-keeping process.

Bill S-33 offers an important opportunity to add a measure of certainty to Canadian evidence law. If further effort is made to address evidentiary issues arising from automated record-keeping practices along the lines we have suggested above, in our view, Bill S-33 will be greatly improved as a result. We, therefore, respectfully offer these comments and recommendations to you for your consideration.



APPENDICE "COMP-2"

L'Association des banquiers canadiens

PROJET DE LOI S-33

LOI FÉDÉRALE DE 1982 SUR LA PREUVE

MÉMOIRE PRÉSENTÉ AU

COMITÉ SÉNATORIAL PERMANENT DES AFFAIRES JURIDIQUES

ET CONSTITUTIONNELLES

MAI 1983

LOI FÉDÉRALE SUR LA PREUVE

I. PRÉAMBULE

Le projet de loi S-33 est une occasion exceptionnelle de réviser la Loi sur la preuve au Canada. Dans le but de contribuer à cette révision, nous désirons porter à l'attention du Comité sénatorial permanent des Affaires juridiques et constitutionnelles nos préoccupations concernant certaines dispositions du projet de loi S-33 relativement aux documents professionnels. Nous estimons que les dispositions du projet de loi S-33 concernant ces derniers passent sous silence diverses questions de la plus haute importance relativement à la preuve et qui concernent les documents intelligibles provenant de l'ordinateur. Pour cette raison, nous craignons que le projet de loi S-33, s'il est adopté, ne perpétue l'incertitude qui règne au sujet de l'admissibilité en preuve de tels documents. La chance de clarifier la loi à cet égard aura été perdue.

II. LE PROBLÈME DE LA PREUVE PRÉALABLE

Depuis des décennies, les documents professionnels des institutions financières font l'objet de règles particulières relativement à la preuve.

Cette situation s'explique du fait que les tribunaux ont reconnu la grande fiabilité des documents professionnels des institutions financières. En raison de l'exactitude de ces documents, il fut stipulé que les officiers des institutions financières ne pouvaient être contraints de témoigner relativement aux éléments y contenus dans les procédures judiciaires.

La Bankers' Books Evidence Act, une loi adoptée par le Parlement du Royaume Uni en 1879, est un exemple de législation spéciale à cet effet. Une disposition équivalente de la législation canadienne, sanctionnée pour la première fois en 1927, se retrouve dans l'article 29 de la Loi sur la preuve du Canada. Cet article stipule qu'une copie de toute inscription dans un livre ou registre tenu dans une institution financière est admise comme preuve prima facie de cette inscription. Un affidavit signé par un directeur de banque attestant que

- 1) le livre ou registre était, lors de l'inscription, l'un des livres ou registres ordinaires de l'institution financière,
- 2) que l'inscription a été effectuée dans le cours ordinaire des affaires,
- 3) que le livre ou registre est sous la garde ou la surveillance de l'institution financière, et
- 4) que cette copie en est une copie conforme, suffit pour la recevabilité en preuve du livre ou registre.

Or, depuis l'adoption de l'article 29, la nature des registres de banques a été considérablement modifiée.

En raison du volume considérable des transactions quotidiennes (plus de cinq millions par jour), les institutions financières canadiennes ont abandonné la tenue manuelle de livres ou de registres en faveur d'un système informatisé et au système d'emmagasiner à long terme des documents, elles ont substitué l'usage du microfilm et des dossiers d'archives sur microfilm. Les documents professionnels sont actuellement informatisés, comme le sont la grande majorité des transactions financières.

S'il est vrai que l'article 29 de la Loi sur la preuve du Canada s'adapte bien aux registres conventionnels, c'est-à-dire ceux où les inscriptions sont faites à la main, des difficultés surgissent lorsqu'on tente d'appliquer cet article aux documents professionnels informatisés. La décision de la Cour d'Appel de l'Ontario dans R.v. McMullen¹ illustre ces difficultés de façon frappante.

Il fut établi dans la cause McMullen qu'une copie des données informatisées provenant de l'ordinateur, relevait de l'article 29, le tribunal ayant déclaré en effet que la copie provenant de l'ordinateur était une copie du document informatisé. Le tribunal ajoutait qu'une preuve de la fiabilité du système informatisé serait requise pour convaincre le tribunal que la copie provenant de l'ordinateur était une "copie véritable" du document professionnel informatisé. Voici ce que déclarait le juge Morden de la Cour d'Appel de l'Ontario:

(1). R. v. McMullen (1978) 100 D.L.R. (3e) 671

"Je conviens que démontrer la fiabilité du document informatisé est un processus plus complexe qu'établir la fiabilité des registres écrits. De plus, j'admets qu'en principe un tribunal devrait examiner attentivement les raisons qui lui sont soumises à l'appui de la fiabilité, comme condition de recevabilité... Il faut prouver à la satisfaction du président du tribunal que les quatre conditions qui apparaissent à l'article 29 ont été remplies. La nature et la qualité de la preuve soumise au tribunal doivent refléter tous faits inhérents à la garde des documents professionnels - dans le cas de documents informatisés, les procédures et le processus relatifs au contenu, à l'emmagasinement des données, à leur retrait et à leur présentation... Si une telle preuve ne peut pas être donnée par le directeur, le comptable, ou l'officier responsable des documents... alors il est clair qu'on ne peut satisfaire aux dispositions de l'article 29 (2) et la preuve du document informatisé sera irrecevable." (p.679)

Une décision plus récente de la Cour d'Appel de l'Ontario dans la cause R v. Bell and Bruce² est un autre cas où un tribunal a dû étudier la question de la recevabilité de documents informatisés.

(2). R. v. Bell and Bruce (1982) 35 O.R. (2e) 164

Dans cette cause, le tribunal a décrété que le document intelligible en question était un original, et non une copie, parce que les éléments du document emmagasinés dans l'ordinateur en avaient été intentionnellement effacés. Le document intelligible provenant de l'appareil étant considéré comme l'original, aucune preuve préalable ne fut requise pour prouver la fiabilité du système informatisé.

En dépit du jugement rendu dans la cause Bell and Bruce, la décision dans la cause McMullen demeure matière de jurisprudence en ce qui concerne la preuve préalable. Par conséquent, la mesure dans laquelle une preuve préalable relativement aux systèmes informatisés est requise pour établir la recevabilité des documents intelligibles provenant de l'ordinateur dans les procédures judiciaires, n'est pas claire. À notre avis, cette question restera sans réponse si le projet de loi S-33 est adopté dans sa forme actuelle, parce que l'article 130 (c) de ce projet fait passer dans la législation la façon dont le problème fut abordé dans la cause McMullen.

L'article 130 (c) du projet de loi déclare qu'un document "original" constitue en partie,

- c) relativement à des données informatisées, tout document intelligible provenant de l'appareil où elles sont emmagasinées et qui les reflète fidèlement ou qui est le produit d'un système qui donne le même résultat.

L'article 130 (c) semble indiquer que pour établir la recevabilité d'un document intelligible provenant d'un ordinateur, il faille démontrer à la satisfaction du tribunal que le document intelligible reflète exactement les données informatisées confiées au système. Pour qu'un document intelligible se conforme aux conditions de l'article 130 (c), il faudrait que des employés de la banque témoignent oralement ou par déclaration sous serment de la fiabilité du système. Le projet de loi ne contient aucun critère quant à la recevabilité des documents intelligibles provenant de l'ordinateur, et il laisse aux tribunaux le soin de définir les critères détaillés pour établir leur authenticité. Etant donné que les tribunaux tiendront compte de la décision rendue dans la cause McMullen pour développer ces critères, l'absence de critères dans le projet de loi lui-même pourrait rendre nécessaire une volumineuse preuve préalable sur la fiabilité du système informatisé.

III. PRÉOCCUPATIONS JUSTIFIÉES

L'Association des banquiers canadiens émet deux réserves importantes sur l'article 130 (c) du projet de loi S-33. En premier lieu, l'absence de toute directive aux tribunaux concernant la preuve préalable relativement aux systèmes informatisés des banques peut constituer une menace à la sécurité de ces systèmes et à la confidentialité des données de la clientèle. En deuxième lieu, le projet de loi S-33 n'indique pas clairement si les preuves à l'appui de la recevabilité de dossiers provenant de l'ordinateur peuvent être présentées par le biais d'une déclaration sous serment d'un employé de banque.

Par conséquent, il pourrait arriver que des employés bancaires soient contraints de témoigner oralement dans des procédures judiciaires n'impliquant pas leur banque. C'est là un inconvénient incompatible avec l'intention que visait le législateur dans l'article 29 de la Loi sur la preuve du Canada et les banques se retrouveraient dans une position analogue à celle qui existait avant 1879.

IV. DANGER POUR LA SÉCURITÉ

À notre avis, en l'absence de dispositions statutaires précises pour protéger la confidentialité des fonctions informatisées, il sera toujours possible de persuader un tribunal de la pertinence d'une information, et celle-ci deviendra par conséquent contraignable, nonobstant le fait que sa divulgation pourrait nuire à la sécurité de l'institution financière. Un tribunal voudrait la réponse à des questions portant sur les méthodes utilisées pour donner accès aux systèmes informatisés, sur le nombre des employés qui peuvent y introduire des éléments ou en retirer, sur le genre de vérifications sécuritaires destinées à empêcher les employés d'abuser de l'information ainsi obtenue, ainsi qu'à un grand nombre d'autres interrogations relatives aux possibilités d'erreurs ou aux actes de malhonnêteté qui pourraient affecter le système informatisé. Si une partie importante des renseignements ainsi requis est portée à la connaissance du public, la sécurité des systèmes mis en place par les institutions financières pourrait être menacée.

Les clients confient aux institutions financières la responsabilité de la sécurité de leurs systèmes. En outre, les tribunaux eux-mêmes reconnaissent que les institutions financières ont le devoir de respecter la confidentialité des données de la clientèle³. Ce devoir est inhérent au fait que les clients fournissent aux institutions financières une vaste quantité d'informations importantes les concernant. Afin de protéger les données de la clientèle et d'empêcher l'accès non autorisé aux systèmes informatisés des institutions financières, tous les éléments du système doivent être entourés de la confidentialité la plus absolue. Pour ce faire, un grand nombre d'institutions financières compartimentent leurs systèmes informatisés en sous-systèmes, dont certains ont seul rôle d'éprouver la sécurité du système principal, alors que d'autres fournissent les éléments de sécurité. Dans nombre de cas, il serait impossible de révéler en détail la façon dont les documents intelligibles provenant de l'ordinateur sont obtenus, sans dévoiler, en même temps, certains détails essentiels au maintien de la sécurité des systèmes.

Il n'existe, dans le projet de loi S-33, aucune restriction sur la divulgation qui peut être exigée d'une institution financière relativement à son système informatisé. Il est clair qu'en certaines circonstances, une institution financière pourrait être forcée à une divulgation susceptible de lui causer un tort.

(3). Tournier V. National Provincial and Union Bank of England,
(1924) I.K.B. 461

V. LE FACTEUR GÊNE

Considéré isolément, l'article 157 du projet de loi S-33 semble reconnaître aux documents professionnels des institutions financières une qualité de preuve analogue à celle que contient l'article 29 de la Loi sur la preuve au Canada, alors que l'article 155 (2) semble requérir une déclaration sous serment lorsqu'une partie fait preuve de l'authenticité ou de l'exactitude d'un document professionnel. Néanmoins, nous craignons que les tribunaux ne considèrent pas la déclaration sous serment comme suffisante pour constituer une preuve préalable relativement à un système informatisé. Cette crainte se fonde sur l'apparente incohérence entre les articles 157 et 155 (2) du projet de loi d'une part et de l'article 130 (c) d'autre part. Il n'est pas clair que la déclaration sous serment soit recevable comme preuve qu'un document intelligible provenant de l'ordinateur "reflète avec exactitude" les données ou l'information confiées au système. Or, si la déclaration sous serment n'est pas recevable, un témoignage oral serait requis pour établir l'authenticité d'un document intelligible provenant de l'ordinateur, ce qui serait contraire à l'objectif fondamental apparent des articles 157 et 155 (2) du projet de loi.

Il s'avérerait déjà gênant pour les employés bancaires d'être contraints à témoigner de l'authenticité des documents professionnels produits à la main, mais le cas serait aggravé dans le cas des documents intelligibles provenant de l'ordinateur.

En effet, dans la plupart des cas, il est presque impossible pour une seule personne de témoigner relativement à un système informatisé dans son ensemble. Pour des raisons de sécurité, une personne peut difficilement connaître un système informatisé en entier. Par conséquent, pour témoigner de la fiabilité du système dans son ensemble, plusieurs employés bancaires seraient contraints de déposer devant le tribunal. De plus, les personnes qui connaissent le système et qui, par conséquent, seraient susceptibles d'être appelées à déposer, ne sont pas des employés d'une succursale locale, mais des employés des centres de données régionaux, du siège social, dont on ne peut se dispenser des services pour des périodes prolongées sans inconvénient sérieux et perte financière pour la banque.

Nous recommandons que le projet de loi S-33 présume de la fiabilité essentielle des systèmes informatisés des banques en acceptant le recours à la procédure de la déclaration sous serment pour les documents professionnels informatisés. D'ailleurs, la fiabilité des systèmes bancaires est prouvée par le volume énorme de transactions qu'ils acceptent chaque jour. Si un système comportait une faiblesse, celle-ci ne tarderait pas à être détectée ou à se manifester. S'il n'est pas indiqué qu'un système était perturbé par un incident le jour ou vers l'époque du soi-disant délit, la preuve devrait être faite que le système fonctionnait conformément à la norme de fiabilité établie à l'article 130 (c).

Pour cette raison, le projet de loi S-33 devrait être rédigé de façon à établir clairement que la procédure de la déclaration sous serment est applicable pour établir l'authenticité des documents professionnels des documents informatisés des institutions financières. De plus, le projet de loi devrait comporter des critères précis, qui seraient suffisants pour établir la recevabilité de documents informatisés par déclaration sous serment. Une institution financière devrait pouvoir satisfaire à ces critères au moyen d'une déclaration sous serment par un représentant de succursale, sans qu'il soit nécessaire de divulguer des informations importantes relativement aux systèmes de l'institution. Si le projet de loi est modifié en tenant compte de ces recommandations, nous estimons que le but essentiel de l'article 29 de la Loi sur la preuve au Canada déjà existante et les articles 157 et 155 (2) de la Loi envisagée, sera atteint, et qu'en même temps sera dissipée toute incertitude quant à la recevabilité et à la valeur en preuve des documents informatisés.

EXEMPLES DE CRITÈRES

Nous trouvons étrange que le projet de loi S-33 accorde si peu d'importance au traitement informatique des données, bien que celui-ci soit au centre de la documentation moderne. D'autres paliers de gouvernement ont établi à l'intérieur de leurs lois des critères précis quant à la recevabilité des documents informatisés.

Les modifications que nous recommandons au projet de loi S-33 ne sont donc pas sans précédent. Par exemple, le rapport du Groupe de travail fédéral/provincial sur l'uniformisation des règlements de la preuve, et sur lequel le projet de loi S-33 est censément fondé, recommande trois critères pour la recevabilité de la preuve informatisée:

1. Preuve que les données à la base du document provenant de l'ordinateur répondent au type de données qui sont ordinairement introduites dans l'ordinateur dans le cours des activités ordinaires de l'organisation de laquelle provient le document;
2. Preuve que les éléments de la banque de données dont est tiré le document ont été introduits dans le cours ordinaire des affaires; et
3. Preuve que la programmation informatisée utilisée dans la production du document reflète fidèlement et de façon juste le contenu de la banque de données.

Même si le troisième critère pourrait avoir pour résultat de livrer à la connaissance du public certains renseignements importants au sujet de la programmation informatisée d'une banque, le Groupe de travail estime, dans son rapport, que le critère pourrait être satisfait en donnant une preuve de la fiabilité de la programmation de l'ordinateur sur une certaine période.

De plus, le Groupe de travail est unanime à recommander que les critères de recevabilité puissent être satisfaits par le biais d'une déclaration sous serment d'authenticité dans les limites des connaissances et du jugement de la personne qui prête le serment.

Un autre exemple de critères relatifs à la recevabilité des documents provenant de l'ordinateur se trouve dans l'article 5 (2) de la Civil Evidence Act du Royaume Uni adoptée en 1968. Cette disposition énumère les critères suivants quant à la recevabilité des documents intelligibles provenant de l'ordinateur, dans les procédures judiciaires:

1. Preuve que le document intelligible provient de l'utilisation ordinaire de l'ordinateur pour les activités exercées;
2. Preuve que l'ordinateur a reçu ordinairement des éléments d'information de la nature de ceux produits;
3. Preuve que l'ordinateur fonctionnait correctement, ou que le bon fonctionnement de l'ordinateur ne fut pas diminué par une opération défectueuse, et,
4. Preuve que l'information a dérivé de celle fournie à l'ordinateur dans le cours normal des activités.

L'addition au projet de loi S-33 de critères semblables à ceux suggérés par le Groupe de travail ou contenus dans la Civil Evidence Act du Royaume Uni ainsi que d'une disposition autorisant clairement que la preuve peut être faite par déclaration sous serment, améliorerait grandement les dispositions du projet quant aux documents professionnels sans atteinte aux droits d'une partie plaidante.

CONCLUSION

Beaucoup de temps et de travail ont été consacrés à la préparation du projet de loi S-33 qui, sans doute, constituera le fondement de la Loi sur la preuve au Canada pour un grand nombre d'années. C'est par conséquent avec regret que nous avons constaté qu'aucune solution n'a été apportée à certains points obscurs de la loi actuelle. Nous avons exprimé nos préoccupations concernant l'absence de critères quant à la recevabilité de documents provenant de l'ordinateur et l'incertitude qui règne à propos de la déclaration sous serment, mais nos questions ne s'arrêtent pas là. Nos doutes persistent, par exemple, au sujet du statut d'un document provenant d'un système à l'intérieur duquel l'original en papier aurait été détruit, ce qui peut se produire dans le cas de la restriction du chèque. Le document est-il un "original" au sens de l'article 130 (c) ou devient-il une "copie" qui doit être traitée selon les dispositions de l'article 133 (a) du projet de loi S-33. Nous avons noté que le projet de loi S-33 ne définit pas le mot "copie" en dépit de l'incertitude attachée à ce mot par suite des décisions dans les causes McMullen et Bell and Bruce, auxquelles nous avons fait allusion. En raison de la fréquence avec laquelle l'information contenue dans des documents originaux est reproduite alors que la documentation originale est détruite, tel que prévu pour le cas des banques aux articles 157 et 159 de la Loi sur les banques, nous prévoyons que d'autres litiges se produiront en raison du fait que le projet de loi S-33 ne tient pas suffisamment compte de ces aspects de la documentation informatisée.

Le projet de loi S-33 constitue une occasion importante d'apporter certains éclaircissements à la Loi sur la preuve au Canada. Nous croyons que ce projet serait grandement amélioré si un effort était fait pour tenir compte de nos suggestions quant à l'admissibilité en preuve des documents informatisés. Nous soumettons respectueusement ces commentaires et ces recommandations à votre considération.



If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESSES—TÉMOINS

From the Canadian Bankers' Association:

Mr. R.M. MacIntosh, President;
Mr. E. Jestin, Supervisor, Internal Control, Evaluation, The
Bank of Nova Scotia;
Ms. Pat Learmonth, Co-ordinator of Communications.

De l'Association canadienne des banquiers:

M. R.M. MacIntosh, Président;
M. E. Jestin, Superviseur, Vérification et évaluation interne,
La Banque de Nouvelle-Écosse;
M^{lle} Pat Learmonth, co-ordinatrice des communications.

HOUSE OF COMMONS

Issue No. 14

Tuesday, May 31, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 14

Le mardi 31 mai 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

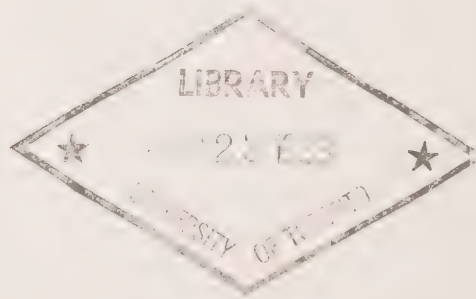
Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

TUESDAY, MAY 31, 1983
(16)

[Text]

The Sub-committee on computer crime met this day at 3:44 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From the Consumers' Association of Canada: Ms. Christine Bisanz, Acting Director of Association and Activities, and Ms. Christine Elliott, Member, Ontario Branch.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15th, 1983, Issue No. 1.*)

Mrs. Elliott made a statement and, with Ms. Bisanz, answered questions.

At 4:45 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MARDI 31 MAI 1983
(16)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h44, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: De l'Association canadienne des consommateurs: M^{lle} Christine Bisanz, directrice suppléante, Politique et activités et M^{lle} Christine Elliott, membre, section Ontario.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

M^{lle} Elliott fait une déclaration et, avec M^{lle} Bisanz, répond aux questions.

A 16h45, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Tuesday, May 31, 1983

• 1543

Le président: Le Sous-comité reprend l'étude de son ordre de renvoi concernant les infractions relatives aux ordinateurs.

Nos témoins aujourd'hui sont de l'Association des consommateurs du Canada. Ce sont M^{lle} Christine Elliott, membre de la section Ontario, et M^{lle} Christine Bisanz, directrice suppléante.

I would like to invite the witnesses to make their statement, and then we will be able to proceed with questions.

Welcome to our committee.

Ms Christine Elliott (Member, Consumers' Association of Canada (Ontario Branch)): Thank you for the opportunity to present the opinions of the Consumers' Association of Canada on the topic of computer theft. I am going to summarize the brief that we submitted earlier.

The Consumers' Association of Canada is a voluntary, non-profit association with 160,000 members located throughout Canada. We have the following objectives: to strengthen consumers through unity in order to improve the standard of living in Canadian homes; to study consumer problems and make recommendations; to bring the views of consumers to the attention of government, trade and industry—provide a channel of communication; and to obtain and provide to consumers information and counsel on consumer goods. Among other activities, we make representations on behalf of consumers to groups such as this—legislatures, courts, administrative tribunals and so forth.

• 1545

We welcome this opportunity to express our views to the subcommittee on computer crime. The establishment of the committee to study a matter which is of particular concern as it affects the principle of individual privacy is an action that we in CAC wholly commend. The computerization of information is increasingly pervasive in our society and, as more and more sophisticated computer technology increases the ability of public and private institutions to store, retrieve, transfer, alter, and otherwise manipulate information at a speed and on a scale unimaginable, we believe consumers have an important stake in this issue. At the same time, the spread of this kind of technology has been paralleled by a substantial and growing documentation of cases of modification or theft of computer programs, software, data, use of computer time, and so forth.

We are very concerned about these phenomena because of our interest and involvement in the development of electronic funds transfer systems. We believe that this kind of system will

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mardi 31 mai 1983

The Chairman: The subcommittee resumes consideration of its order of reference concerning computer crime.

Our witnesses today are representatives of the Canadian Consumers Association. May I introduce Ms Christine Elliott, Member, Ontario Branch, and Ms Christine Bisanz, Acting Director.

Je demanderai aux témoins de faire leur exposé et nous passerons ensuite aux questions.

Bienvenue au Comité.

Mlle Christine Elliott (membre, Association des consommateurs du Canada (Section Ontario)): Merci de nous donner l'occasion d'exprimer le point de vue de l'Association des consommateurs du Canada au sujet des infractions relatives aux ordinateurs. Je vais résumer le mémoire que nous vous avons déjà présenté.

L'Association des consommateurs du Canada est une association bénévole sans but lucratif qui regroupe 160,000 membres au Canada. Nos objectifs sont les suivants: unifier les consommateurs pour améliorer le niveau de vie dans les foyers canadiens, étudier les problèmes des consommateurs et faire des recommandations, présenter le point de vue des consommateurs au gouvernement et aux entreprises, offrir un canal de communication, obtenir pour l'offrir aux consommateurs des renseignements et des conseils concernant les biens de consommation. Nos activités nous amènent à faire des démarches au nom des consommateurs auprès de groupes comme celui-ci, des assemblées législatives, des tribunaux administratifs ou autres.

Nous sommes heureux d'avoir l'occasion d'exprimer notre point de vue devant le sous-comité sur les infractions relatives aux ordinateurs. La formation d'un comité pour étudier une question aussi cruciale en ceci qu'elle touche la vie privée des particuliers est une mesure dont se félicite l'A.C.C. De plus, dans notre société, on constate que des renseignements sont mis sur ordinateur, et nous pensons que ce phénomène concerne les consommateurs au premier chef, étant donné que les techniques informatiques de plus en plus poussées permettent aux institutions publiques et privées d'emmagasiner, de récupérer, de transmettre, de modifier, bref de manipuler ces renseignements sur une grande échelle et à une vitesse inimaginable. En même temps, on a constaté qu'à mesure que les techniques se répandaient, on rapportait de plus en plus de cas où les programmes informatiques, le logiciel et les données étaient altérés, ou encore volés, et où il y avait abus du temps informatique.

Nous nous inquiétons de ces phénomènes parce que nous nous occupons de très près de l'évolution des systèmes électroniques de virement de fonds. Nous pensons que ce genre de

[Texte]

increase the vulnerability of computerized data to theft, to fraud, and to invasion of privacy, which is of enormous concern to the association. To the extent that this is the case, we are afraid that ordinary Canadian consumers will frequently be indirectly the victims of computer crime and invasion of privacy.

Generally privacy is a well-accepted concept in search of a really precise legal definition. Efforts to nail down a specific legal doctrine have always been confounded by the evolution of technology. Every time something changes, a new threat seems to arise. Back in 1890 in the United States, when Brandeis and Warren were writing about invasion of privacy, they were really responding to . . . the catalyst was a series of technological innovations in those days, the telephone, audio recorder . . .

Privacy cannot really be viewed in narrow terms with complete security or a computer crime but, really, in terms of consumerism in computers. It is an important aspect of a consumer's relationship with the system and with any kind of transaction they make. Computing and computers in combination with new telecommunications systems and user-friendly technology is, or will be, quite commonplace. These systems generally entail many transactions, many users, and a great deal of personal information is generally provided to complete that transaction. In order to obtain a service or a good, a consumer usually hands over more than just money. They usually hand over personal information, and that has a value as well. Information about financial well-being, credit, purchasing habits, hobbies, interests, any of a wide range of material has to be proffered to gain credit or even to get service for an item or a purchase.

The consumer is really on the front line of this data exchange. He is on the front line of the computer revolution, you could say; he is an information provider and an information user. A simple example, I think, can illustrate the impact the computer will have on dealing with personal data in a consumer's transaction. In the past, property purchased in Ontario usually entailed a title search. A potential purchaser's agent went to a county or municipality and located details about a piece of property that they were going to purchase or buy through an agent. It was really a paper or manual search.

Today, Ontario is introducing the Real Property Documents and Recording Act. It is currently under draft. This will essentially computerize all that information about property. However, in the supporting documentation to this legislation, you find that the user will be able to locate property by an owner's name. So you would be able to put in somebody's name and find out all the property by county which that person owns or even may have mortgaged or be the mortgagee of.

[Traduction]

système agumentera la possibilité de vols de données informatisées, de fraudes en général, d'empiètement sur la vie privée, ce dont se préoccupe au plus haut point l'association. Ainsi, nous craignons que les consommateurs canadiens moyens soient fréquemment, indirectement, les victimes d'infractions relatives aux ordinateurs et d'empiètement sur leur vie privée.

Le droit à la vie privée est une notion en général bien comprise bien qu'elle ne soit pas encore définie précisément du point de vue juridique. L'évolution des techniques a toujours rendu désuets les efforts consentis pour cerner cette notion de façon précise du point de vue juridique. Chaque fois qu'il y a un changement, une nouvelle menace surgit. En 1890, aux États-Unis, quand Brandeis et Warren parlaient d'empiètement sur la vie privée, ils répondaient à une situation créée par les innovations technologiques de l'époque, le téléphone, le magnétophone . . .

La vie privée ne peut pas être vraiment envisagée du point de vue restreint de la sécurité totale ou du point de vue des infractions rendues possibles par les ordinateurs, mais plutôt du point de vue de la consommation qui caractérise les ordinateurs. La vie privée est un aspect capital des rapports entre le consommateur et le système, et de toutes les transactions. Les ordinateurs et l'informatique assortis des nouveaux systèmes de télécommunication et de la technologie facile d'accès sont déjà courants ou le seront. Ces systèmes en général permettent des transactions multiples, des abonnés multiples et beaucoup de renseignements personnels sont fournis en général chaque fois qu'il y a une transaction. Quand il s'agit d'acquérir un service ou un bien, le consommateur d'habitude donne plus que de l'argent. Il doit donner des renseignements personnels qui ont eux-mêmes une valeur. Il doit donner des renseignements sur sa situation financière, son crédit, ses habitudes d'achat, ses passe-temps, ses intérêts, et beaucoup de détails doivent être fournis pour obtenir du crédit, un service ou un bien.

Le consommateur se trouve donc véritablement en première ligne lors de cet échange de renseignements. Il est en effet dans la révolution électronique, car il est à la fois fournisseur et usager des renseignements. Je puis vous donner un simple exemple qui illustre l'impact de l'ordinateur quand des renseignements personnels sont fournis lors d'une transaction. Dans le passé, quand on achetait une propriété en Ontario, il fallait vérifier les titres de propriété. L'acheteur éventuel envoyait quelqu'un au registre du comté ou de la municipalité, qui devait recueillir tous les détails sur la propriété qu'on envisageait d'acheter. Il s'agissait d'une recherche manuelle, dans la paperasse.

Aujourd'hui l'Ontario envisage de faire adopter la *Real Property Documents and Recording Act*. Le projet de loi est en cours de rédaction, et il permettra de mettre sur ordinateur tous ces renseignements concernant la propriété. Néanmoins, dans les documents afférents à la loi, on apprend que l'utilisateur pourra avec le nom du propriétaire repérer n'importe quelle propriété. Il suffira de donner le nom du propriétaire à l'ordinateur et vous trouverez quels sont les propriétés, suivant le comté, qu'il possède ou encore celles dont il est le créancier ou le débiteur hypothécaire.

[Text]

If you had wanted to obtain this kind of information previously, it would have meant a mammoth paper search. You would have had to go to every county and go through every book of property to locate the specific person's name. You may, or may not, think that is an invasion of privacy, but I think it does illustrate, in a consumer transaction, the kind of ease with which you will be able to obtain information which previously was not readily available. That was really just to illustrate what the consumer is facing now.

New technologies are especially of concern to the Consumers' Association of Canada, especially two-way to a television, for example, electronic funds transfer, and this includes automatic banking, electronic mail, point-of-sale transactions. All these do not appear to us to be well dealt with in existing legislation, from the viewpoint of privacy. System and data security is really unaddressed in law to that extent, at least on a consistent basis. The ability to collect and transfer, and especially correlate large amounts of personal information at what is a relatively insignificant cost means that inadequate security and poor regulatory control can really allow unheard of breaches of confidentiality and, in fact, amassing of information. In some cases the issue really is not malice, it is really negligence. Some provinces have enacted data bank leakage legislation but widespread review and regulation of security of data banks and transmission systems is virtually non-existent in Canada.

• 1550

Another issue of importance to the Consumers Association, too, is the fate of such data banks under disaster scenarios; war, civil disruption, natural disasters. Once again, the ability to locate people by specific characteristics such as race or religion is rather frightening, especially to people who lived through the Second World War. In fact, we are led to share the observation of a study commissioned by the Ontario government in 1978 that the right to privacy is an illusion in the legal sense for there is no such right. In the past, there has been no real need for legally guaranteed right to privacy, but electronic funds transfer and other developments are forcing upon our society the need for some form of protection of the individual from the computer.

Personal information has always been of value to others as well as to the individual to whom it pertains. However, the cost of obtaining that information in a usable form, not to speak of sheer physical barriers, generally precluded any large-scale attempts before the advent of efficient copying devices, such as cameras and photocopiers. Information still had the status of a thing, because it was contained in a discrete and unique unit. Other characteristics of that data were its generally wide scatter; its cumbersomeness and its likelihood of being rapidly obsolete. Trespass, theft and fraud were often necessary to obtain that information.

[Translation]

Autrefois, pour obtenir ces renseignements, il fallait des recherches très poussées. Il fallait se rendre dans tous les comtés, consulter tous les cadastres pour retrouver le nom du propriétaire. Vous n'êtes pas obligés de reconnaître qu'il s'agit là d'une intrusion dans la vie privée, mais cela démontre comment à l'occasion d'une transaction, désormais il sera de plus en plus facile d'obtenir des renseignements, qui autrefois étaient difficiles à trouver. Voilà donc un exemple de ce qui attend le consommateur désormais.

Les nouvelles techniques inquiètent particulièrement l'Association des consommateurs du Canada, surtout la télévision bi-directionnelle, par exemple, et les virements électroniques de fonds, et cela inclut les guichets automatiques, le courrier et les transactions commerciales électroniques. Nous pensons que toutes ces questions ne sont pas bien couvertes dans la loi actuelle, du point de vue de la protection de la vie privée. Il n'existe pas de disposition législative ordonnée concernant la sécurité des données et des systèmes. Qu'il soit possible d'amasser et de transmettre, mais surtout de jumeler de grandes quantités de renseignements personnels à un coût relativement infime, témoigne de la sécurité insuffisante et de la lacune réglementaire qui peuvent ouvrir la porte à des indiscrétions inouïes et en fait à l'accumulation de renseignements. Dans certains cas, ce n'est pas dans une intention malhonnête, mais tout simplement par négligence. Certaines provinces ont adopté des Lois sur les fuites de données informatisées, mais au Canada, il n'existe pour ainsi dire pas d'examen général et de réglementation de la sécurité des banques de données et des systèmes de transmission.

Pour l'Association canadienne des consommateurs du Canada, il est inquiétant aussi de songer à ce qu'il adviendra de ces banques de données en cas de catastrophe comme une guerre, un soulèvement ou une catastrophe naturelle. Une fois de plus, le fait que l'on puisse retracer des gens suivant leur race ou leur religion est plutôt alarmant notamment pour les gens qui ont vécu la deuxième guerre mondiale. En fait, nous partageons une remarque faite dans une étude pour le compte du gouvernement de l'Ontario en 1978. Le droit à la vie privée est une illusion du point de vue juridique parce qu'il n'existe pas. Dans le passé, le besoin ne s'est pas fait sentir de garantir ce droit sur le plan juridique, mais les virements électroniques de fonds et d'autres développements forcent notre société à chercher une protection pour le particulier contre l'ordinateur.

Les renseignements personnels ont toujours eu une certaine valeur pour ceux qu'ils concernent comme pour les autres. Néanmoins, le coût pour rendre ces renseignements utilisables, sans compter les obstacles matériels tout simplement, ont empêché en règle générale qu'on essaie d'obtenir ces renseignements sur une grande échelle jusqu'à ce que nous connaissions des photocopieuses et des appareils photos plus efficaces. Ces renseignements étaient encore considérés comme des objets parce qu'ils se trouvaient sous une forme unifiée et discrète. À cette époque-là, certains renseignements étaient en général dispersés, encombrants, et rapidement, ils devenaient périmés. Pour les obtenir, il fallait les voler, les obtenir frauduleusement ou en pénétrant par infraction.

[Texte]

Electronic data processing and telecommunication systems have really removed a lot of those physical barriers to information collection and our legal system, in some cases, has been too archaic to respond. The capacity of our new technology to store and to correlate information by individuals is large and is growing.

Two-way television is an excellent example where a service in conjunction with other electronic communications and data transfer systems to the subscriber are really enormous. Home shopping, banking; you can be polled on your opinions about political parties or other issues. You can study; you can donate to charitable programs; you can do your banking; you can buy something. A massive amount of data about a specific individual or household can be obtained by cable utility. For example, what you buy and how you pay for it; whether you are at home and what time you got home. I quote Ann Cameron from the University of New Brunswick:

The accumulation of massive data bases concerning individuals from communications networks can present a very serious threat to current notions of privacy... Data which might previously have been considered to be non-sensitive can now become quite sensitive because of the correlation... Since such data bases can easily be transferred between systems, issues of data security and thus information privacy become complex and difficult.

Computer theft and fraud are neither insignificant nor unnoticed within or without the computer industry. You merely need to review existing publications in the computer industry to see the large number of articles and interest evinced in this particular area. To quote one authority on the subject:

Aspects of computer crime include theft or modification of computer programs, theft of computer time, theft of property through use of computers... Outsiders also may be able to telephone their way into computer systems... Even organized crime appears to be getting into the act. The risk of being caught, let alone prosecuted and convicted, is very low.

EFTS will, in many people's opinion, really provide a field day, because security problems are really significant in such a widespread system network, where you might even link up home systems, point-of-sale systems in retail outlets, banks... a whole wide range of services can be linked together.

Many Canadian consumers are becoming more concerned about the issues of privacy and electronic funds transfer and other telecommunications systems. In March of 1982, the London local of the Consumers Association presented a seminar on EFTS. Of all the many issues which came up concerning consumers, one of the most important was considered to be the issue of privacy—the protection of financial privacy, which can not be waived. This issue, in conjunction with concern about unauthorized use of transaction cards,

[Traduction]

Le traitement électronique des données et les systèmes de télécommunication ont donc supprimé beaucoup de ces obstacles matériels, et notre régime juridique, dans certains cas, est désuet. Les particuliers ont toute capacité, et cela ne fait que s'accroître grâce à la nouvelle technologie, d'emmagasiner et de jumeler des renseignements.

La télévision bidirectionnelle est un excellent exemple, car on offre un service gigantesque à l'abonné en le reliant à d'autres systèmes de transmission électronique de données et de communications. Les opérations bancaires, les transactions commerciales à la maison, les sondages d'opinion sur les partis politiques ou d'autres sujets, les études, les dons charitables, tout est possible désormais. Les sociétés de câble peuvent obtenir des quantités massives de renseignements sur des particuliers comme sur des ménages. Par exemple, ce que vous achetez et comment vous le payez. À quelle heure vous rentrez à la maison et combien de temps vous y restez. Je vais vous citer l'étude de Anne Cameron de l'université du Nouveau-Brunswick:

Les réseaux de communications qui accumulent des bases de données considérables concernant les particuliers constituent une menace grave contre la notion de vie privée telle que nous la connaissons actuellement... les données qui autrefois n'étaient peut-être pas considérées comme personnelles, peuvent le devenir à cause du jumelage qu'on en fait... puisque les bases de données peuvent être transmises facilement entre les systèmes, la sécurité des données et par conséquent le caractère privé des renseignements deviennent complexes et difficiles.

Le vol et la fraude électroniques ne sont ni infimes ni imperceptibles à l'intérieur comme à l'extérieur de l'industrie de l'informatique. Il suffit de voir ce que publie l'industrie de l'informatique pour se rendre compte de l'intérêt que suscite le sujet. Les articles là-dessus sont nombreux, et je vous citerai une sommité en la matière:

Les infractions relatives aux ordinateurs comprennent le vol ou la modification de programmes d'ordinateur, le vol du temps d'ordinateur, le vol d'autres objets au moyen d'ordinateurs... on peut arriver à téléphoner à un système d'ordinateur... même le crime organisé semble y venir. Il y a peu de chance de se faire prendre, encore moins d'être poursuivi et condamné.

Les systèmes électroniques de virement de fonds seront, de l'avis de plusieurs, un cas-type, car les problèmes de sécurité sont considérables, étant donné que le réseau est vaste, et que l'on peut y intégrer des systèmes résidentiels, des systèmes de transactions commerciales électroniques situées dans des magasins de détail, des banques, toute une gamme de services.

Beaucoup de consommateurs canadiens se préoccupent de la vie privée, des virements électroniques de fonds et des autres systèmes de télécommunication. En mars 1982, la section de London de l'Association canadienne des consommateurs a présenté un séminaire sur les effets des virements électroniques de fonds. De toutes les nombreuses questions concernant les consommateurs, il a été considéré qu'une des plus importantes était celle de la vie privée, la protection des renseignements financiers à laquelle on ne peut renoncer. Cette question, avec

[Text]

really rated the highest in all of our seminar participants' concerns.

• 1555

Consumers have a responsibility, too, of course, for the intelligent review of their own data or personal information provision. Inger Hansen, the Privacy Commissioner, believes that consumers should ask the following questions: Do you need to know? Why do you need to know? How will you use my personal information? With whom will you share it? And for the purposes here, the question: What measures will you take to keep it secure, confidential, accurate, relevant, and up to date?

Studies undertaken by researchers such as David Flaherty, at the University of Western Ontario, suggest that consumers really are not that well informed and somewhat open. They are newly confronted with technological development, and incidents of breaching of confidentiality are not well-known or well documented at the moment. Clearly, more information about privacy, and how it interfaces with data collection systems is vital.

For its part, the Consumers Association has had a history of action and advocacy in this field. In 1973 we passed a resolution regarding the privacy of the individual, and in 1979, CAC passed a resolution regarding social insurance numbers, which stated in part that the Consumers Association requests the government to provide adequate safeguards for the protection of the privacy of individuals in any system for administering the use of social insurance numbers. In our brief to the Privacy Commissioner in April 1980, we commented on the use of SIN, and expressed concern about the possible abuse of information of the private sector, if SIN was allowed in there. There must be guidelines and regulations to effectively protect the individual's right to privacy.

CAC has reviewed much of the information regarding EFTS, and the issue of information privacy, and we will be proposing resolutions to the Consumers Association of Canada's annual meeting in Halifax. We will be addressing these issues.

CAC is confident that this subcommittee will examine these matters as they relate to protecting personal privacy. Specifically, we recommend:

(a) that the committee recognize the need to amend the Criminal Code of Canada to make the unauthorized appropriation, conversion, removal, destruction, or manipulation of computer services facilities or data bases a criminal offence;

(b) that they recognize the need for the establishment of standards for the confidentiality and security of client data for

[Translation]

celle de l'utilisation non autorisée des cartes de transactions, a occupé la tête de liste des préoccupations de tous les participants de nos séminaires.

Bien entendu, les consommateurs ont également la responsabilité d'exercer un contrôle intelligent sur leurs propres données ou sur les renseignements personnels qu'ils fournissent. Inger Hansen, le commissaire à la vie privée, croit que les consommateurs devraient poser les questions suivantes: Est-ce vraiment nécessaire? Pourquoi voulez-vous le savoir? Comment utiliserez-vous ces renseignements personnels? A qui les communiquerez-vous? Et dans le cas qui nous intéresse tout particulièrement, la question suivante: Quelles mesures prendrez-vous pour vous assurer que ces renseignements sont exacts, pertinents et quelles mesures prendrez-vous pour les protéger, respecter leur caractère confidentiel et les tenir à jour?

Des études menées par des chercheurs tels que David Flaherty de l'Université de *Western Ontario*, suggèrent que les consommateurs ne sont vraiment pas bien informés. Ils sont confrontés à une technologie nouvelle et les exemples d'utilisation non autorisée de ces renseignements sont insuffisamment connus ou insuffisamment rapportés pour le moment. Il est absolument vital qu'une plus grande publicité soit faite sur les conséquences de l'informatique sur la vie privée.

Pour sa part, l'action de l'Association des consommateurs dans ce domaine est déjà ancienne. En 1973, nous avons adopté une résolution relative au droit à la vie privée des particuliers, et en 1979, une résolution relative aux numéros d'assurance sociale, réclamant entre autres au gouvernement des mesures assurant de façon efficace la protection de la vie privée des particuliers dans tout système utilisant ces numéros d'assurance sociale. Dans notre mémoire soumis au commissaire à la vie privée en avril 1980, nous commentons l'utilisation des numéros d'assurance sociale et signalions la possibilité d'abus dans le secteur privé si on lui permettait d'utiliser ces numéros. Des directives et des règlements protégeant effectivement le droit à la vie privée des particuliers sont indispensables.

Nous avons revu une grande partie de la documentation concernant les virements électroniques dans le contexte des renseignements confidentiels qui sont fournis et nous proposerons des résolutions lors de notre conférence annuelle à Halifax. Ces questions seront à l'ordre du jour.

Nous sommes convaincus que votre Sous-comité étudiera l'incidence de ces questions sur la protection de la vie privée. Plus particulièrement, nous recommandons:

a) que votre Comité reconnaisse la nécessité de modifier le Code criminel du Canada pour que l'appropriation, la conversion, la suppression, la destruction ou la manipulation non autorisée de services informatisés ou de données informatisées soient considérées comme une infraction criminelle;

b) que vous reconnaissiez la nécessité d'instituer des normes de protection et d'utilisation des données fournies par les clients à

[Texte]

both privately- and publicly-controlled personal data systems, and to develop a mechanism for monitoring compliance;

(c) that they recognize the importance of urging the Government of Canada, in conjunction with industry, consumer, professional, and other relevant groups to undertake to inform consumers of their rights and responsibilities;

(d) that they recognize the need to entrench the right to individual privacy in the Charter of Rights and Freedoms.

We sincerely hope that these issues will be addressed, and that both the federal and provincial levels of government will see the need for effective computer crime and privacy legislation. We believe that protection is vital to Canadian consumers. Thank you.

The Chairman: Thank you. Time for questions. Mr. Robinson?

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman. Starting with the last first, it seems to me that the basis of your brief really is the right to privacy per se, and not necessarily computer crime; that you are, I assume, endeavouring to relate privacy to the computer crime issue that we are concerned with.

Ms Elliott: Well, we believe that the access to personal information has been greatly facilitated by computerization and telecommunications systems, and the personal information which previously was not sensitive because it was just aggregated, becomes sensitive. That is the issue we are concerned with when it comes to computer theft.

Mr. Robinson (Etobicoke—Lakeshore): In trying to determine your major concern, it seemed to me that first of all, you were concerned about the unknown. And I guess we all are because we are in a rapidly advancing kind of electronic age, where the computer is concerned. Also, you seem to show considerable concern about the rapid development of electronic funds transfer systems. This seems to be a real focus that you have. Then there is the whole question of the invasion of privacy as brought about through what I think you call "computer revolution". What do you see as an overall control mechanism for computer crime? Is it something like changing statute law? Is it having a code of ethics? Are there some other criteria you think should be utilized that are not presently being considered?

• 1600

Ms Elliott: We would like to see it dealt with, really, at both ends. On one side we believe personal information in data and information is of value and should be defined as property. Therefore, unauthorized access or utilization should be defined as theft of that property and, on that basis, it should come under the Criminal Code.

On the other side of the system, we are suggesting that some sort of voluntary standards put together by industry, consumers, government be established, so that computer systems' data

[Traduction]

des systèmes informatisés aussi bien privés que publics et de mettre en place une procédure de contrôle;

c) que vous reconnaissiez l'importance de réclamer au Gouvernement du Canada, en conjonction avec l'industrie, les consommateurs, les professionnels et les autres groupes intéressés, qu'il s'engage à informer les consommateurs de leurs droits et de leurs responsabilités;

d) que vous reconnaissiez la nécessité de consacrer le droit à la vie privée des particuliers dans la Charte des droits et libertés.

Nous espérons sincèrement que ces questions seront étudiées et que les gouvernements fédéral et provinciaux comprendront la nécessité d'une véritable loi sur les infractions relatives aux ordinateurs et sur la vie privée. Nous croyons que pour les consommateurs canadiens, cette protection est vitale. Merci.

Le président: Merci. Nous passons aux questions. Monsieur Robinson?

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président. Commençant par la fin, il me semble que votre mémoire porte avant tout sur le droit à la vie privée en tant que telle et non pas nécessairement sur les infractions relatives aux ordinateurs; que vous vous efforçez, je suppose, de lier la défense du droit à la vie privée à la question des infractions relatives aux ordinateurs dont nous sommes saisis.

Mme Elliott: Nous croyons que l'accès aux renseignements personnels a été grandement facilité par l'informatique et la télématique et que ces renseignements qui, auparavant, ne présenteraient pas de risques parce que dispersés, en présentent un maintenant. C'est ce problème qui nous inquiète, s'agissant de truanquie.

M. Robinson (Etobicoke—Lakeshore): En essayant de déterminer votre inquiétude principale, il m'a semblé tout d'abord que ce qui vous inquiétait le plus, c'est l'inconnu. Je suppose qu'il en va de même pour tout le monde car nous entrons rapidement dans l'ère de l'électronique, dans l'ère de l'informatique. Vous semblez également vous inquiéter considérablement de l'évolution rapide des systèmes de virement électronique. Vous semblez beaucoup insister là-dessus. Ensuite il y a toute la question de l'invasion de la vie privée provoquée par la «révolution informatique», comme vous l'appellez, si je ne m'abuse. Quels moyens de contrôle général de la truanquie proposez-vous? Une modification de la législation? Un code de déontologie? Y a-t-il d'autres critères auxquels on ne songe pas actuellement, et qui devraient, selon vous, être utilisés?

Mme Elliott: En réalité, nous aimerions voir une action simultanée en amont et en aval. D'une part, nous croyons que les renseignements personnels ont une valeur et que la définition de propriété devrait leur être appliquée. Par conséquent, l'accès ou l'utilisation non autorisé devrait être considéré comme un vol et par là même tomber sous le coup du Code criminel.

D'autre part, nous suggérons l'institution de normes volontaires fixées à la fois par l'industrie, les consommateurs et le gouvernement afin que les banques de données informatisées

[Text]

banks have an established standard with which to measure their own security systems. Not all data banks are as sensitive, or as large, or require the same kind of security background that others do, so we are recommending that.

Mr. Robinson (Etobicoke—Lakeshore): When we had the Bankers' Association before us—last week, I guess it was—they indicated that they had very little concern about computer theft. I think part of it was because they felt that they had internal management control and they had a sophisticated setup of safeguards and security such that they did not really think they had a problem. But I am wondering, are the great numbers out there that do not have this elaborate security, this sophisticated system, the ones you are really concerned about—that is, little Mr. and Mrs. Consumer?

Ms Elliott: I think—the CAC thinks—this is a responsibility on both sides. If you use the bankers' analogy, I am sure they make every effort to ensure that their vaults are secure and they have property security systems; they would not suggest for a minute that theft of money from their vaults should not be punished under the Criminal Code. I would say that the same kind of analogy applies to the information they hold in their data bank. I have not read any information, or come across any articles that suggest for a second that any kind of telecommunications, especially a widespread one like EFT, are not vulnerable to outside access.

Mr. Robinson (Etobicoke—Lakeshore): Do you feel that there should be compulsory reporting of computer crime? If there has been access to or trespass in your data bank and you have knowledge of this, do you feel that there should be compulsory reporting?

Ms Elliott: I am afraid I would have to think about that. My top of the head response would be that I assume that if companies have a lot of investment in their computer systems, if they want to encourage some sort of belief in the inviolability of their systems, they would want to encourage any kind of mode by which they could discourage access. So, yes, they should be reporting it.

Mr. Robinson (Etobicoke—Lakeshore): All right. Then you are suggesting that there could be amendments to the Criminal Code, therefore, there would be offences under the Criminal Code and, in order to have offences, somebody needs to inform. You would then, I suppose, suggest that whoever obtains the information to the effect that there has been computer theft or access should, in fact, relate this to the police authorities and have the person or persons charged.

Ms Elliott: I would say the same kinds of criteria that apply to any kind of crime should apply to this one. I do not know why it would be treated differently.

Mr. Robinson (Etobicoke—Lakeshore): That brings up another question, that of the definition of property. I think in your statement, along with that, you talk about information and you indicate that information is not a thing, as required

[Translation]

évaluent leur propre système de sécurité en fonction d'une norme agréée. Toutes les banques de données ne sont pas aussi sensibles ou aussi importantes ou ne nécessitent pas les mêmes mesures de sécurité, et c'est la raison pour laquelle nous faisons cette recommandation.

M. Robinson (Etobicoke—Lakeshore): Lorsque les représentants de l'Association des banquiers sont venus témoigner la semaine dernière, je crois, ils nous ont dit qu'ils accordaient fort peu d'importance à ces délits. En partie, je crois, parce qu'ils estimaient avoir en place des systèmes de contrôle interne, de protection et de sécurité suffisamment perfectionnés pour ne pas véritablement les considérer comme un problème. Je me pose cependant la question suivante. La grande majorité de ceux qui n'ont pas ces systèmes de sécurité et de protection perfectionnés, ceux pour lesquels vous avez véritablement des inquiétudes, est-ce que ce ne sont pas justement M. et M^{me} Consommateur?

Mme Elliott: Je pense, notre association pense, que la responsabilité est partagée. Reprenant l'analogie des banquiers, je suis certaine qu'ils font tous les efforts pour s'assurer que leurs coffres-forts sont inviolables et ils possèdent des systèmes de sécurité; ils ne suggéreraient pas un instant que voler de l'argent dans leurs coffres-forts ne devrait pas être puni par le Code criminel. J'estime que le même genre d'analogie s'applique aux renseignements qu'ils détiennent dans leurs banques de données. Je n'ai jamais trouvé un seul article suggérant un instant que les réseaux de télécommunication, surtout les réseaux aussi étendus que ceux des virements automatiques, sont inviolables.

M. Robinson (Etobicoke—Lakeshore): Pensez-vous qu'il devrait être obligatoire de rapporter toute infraction relative à des ordinateurs? S'il y a eu accès non autorisé aux données contenues dans votre ordinateur et que vous le sachiez, devrait-il être obligatoire de le rapporter?

Mme Elliott: Il faudrait que j'y réfléchisse. Ma première réaction serait de supposer que les compagnies ayant investi de gros capitaux dans l'informatique doivent souhaiter que l'on croit à l'inviolabilité de leur système et, par conséquent, encourager tout moyen décourageant l'accès non autorisé. Rapporter ces infractions devrait donc être obligatoire.

M. Robinson (Etobicoke—Lakeshore): Très bien. Vous suggérez ensuite une modification du Code criminel et, par conséquent, ces délits tomberaient sous le coup du Code criminel. Pour qu'il y ait délit, il faut que quelqu'un le rapporte. Je suppose que vous suggéreriez alors que quiconque apprend qu'il y a eu vol ou accès non autorisé devrait rapporter ce fait aux autorités policières et faire inculper le ou les responsables.

Mme Elliott: Les mêmes genres de critères s'appliquant à tout autre crime devraient également s'appliquer dans ce cas. Je ne vois pas pourquoi il faudrait faire une différence.

M. Robinson (Etobicoke—Lakeshore): Cela me conduit à une autre question, celle de la définition de propriété. Dans votre exposé, vous parlez de renseignements et selon vous, les renseignements ne sont pas un objet, ce que réclame le Code

[Texte]

under the Criminal Code. Do you feel there should be some amendment here? How could this be corrected?

Ms Elliott: In common law, it is the specific thing. Yes, we think it should be defined as property and subject to theft. For example, at present if you copied payroll records—and there is a documented example of this—you would not be charged with theft, because the value of the item that you have taken, especially since it is a copy, is at most the value of the paper. We would suggest that that should be further defined as property and that . . .

Mr. Robinson (Etobicoke—Lakeshore): You would say that there is an intrinsic value here that should be considered as having much more value than just the paper that it is copied on.

Ms Elliott: Yes—personal information of value.

Mr. Robinson (Etobicoke—Lakeshore): You have indicated a great deal of concern about the right to privacy and the fact that it is not entrenched in the Charter of Rights and Freedoms, but I would suggest to you that the common law provides many protections, which, in my view, are not outmoded by the Charter of Rights and Freedoms. For instance, we have safeguards like *habeas corpus* and other writs and many common law provisions. They are still in place.

• 1605

Ms Elliott: Generally, you have to be in the midst of some sort of action; and shall we say that, in common law, the definition of privacy or the idea of invasion of privacy is not generally accepted. But it is not generally rejected, either; and you can follow through case law that shows some support for the idea.

Our suggestion that it be entrenched in the Charter of Rights and Freedoms is that many people believe it is a generally accepted right, and there is some case precedent that suggests the courts would view it in that way. This is our attempt to suggest it should be generally acknowledged.

Mr. Robinson (Etobicoke—Lakeshore): If we have a Privacy Act that covers this, why do we need to entrench it in the Charter of Rights and Freedoms?

Ms Elliott: Many rights that are entrenched in the Charter of Rights and Freedoms also have parallel legislation associated with them. I do not see that there is any conflict there.

Mr. Robinson (Etobicoke—Lakeshore): I am not talking about the conflict. I am talking about the need of having it enshrined in the Charter of Rights and Freedoms when you already have a Privacy Act. I might question a number of other matters that are also in the Charter of Rights and Freedoms, when we have other legislation or other safeguards as well.

Ms Elliott: Our Privacy Act, I believe, deals currently with the federal right to government information. It does not deal with private information. However, back to computers, back to

[Traduction]

criminel pour ces définitions. Devrait-on modifier la loi? Comment le faire?

Mme Elliott: En common law, c'est la chose elle-même. La définition de propriété devrait leur être appliquée et donc la notion de vol. Par exemple, à l'heure actuelle si vous copiez le fichier du personnel d'une entreprise—et il existe un exemple à ce sujet—vous ne pouvez être accusé de vol car la valeur de ce que vous avez pris, surtout puisqu'il ne s'agit que d'une copie, est au plus la valeur du papier. La définition de propriété devrait y être appliquée et . . .

M. Robinson (Etobicoke—Lakeshore): Selon vous, la valeur intrinsèque de ce document devrait être considérée comme supérieure à la valeur du simple papier sur lequel il a été recopié.

Mme Elliott: Oui—des renseignements personnels ayant de la valeur.

M. Robinson (Etobicoke—Lakeshore): Vous insistez fortement sur le droit à la vie privée et sur le fait qu'il n'est pas consacré dans la Charte des droits et libertés, mais je me permettrais de vous signaler que la *common law* prévoit de nombreuses protections qui, à mon avis, n'ont pas été déplacées par la Charte des droits et libertés. Nous avons des protections comme par exemple, l'*habeas corpus*, divers brevets et de nombreuses règles de *common law*. Elles existent toujours.

Mme Elliott: De façon générale, elles ne peuvent être invoquées que dans le cadre d'une action en justice, et nous pourrions dire que la *common law* ne reconnaît généralement pas la définition de la vie privée ou le concept d'invasion de la vie privée. L'idée n'est pas non plus rejetée et on peut en voir une certaine consécration dans la jurisprudence.

Nous avons proposé que ce soit enchâssé dans la Charte des droits et libertés parce que beaucoup de gens croient qu'il s'agit d'un droit généralement accepté et certains précédents montrent bien que les tribunaux sont de cet avis. Nous avons donc tenté de proposer que ce droit soit reconnu.

M. Robinson (Etobicoke—Lakeshore): Si nous avons une Loi sur la protection des renseignements personnels qui en tient compte, pourquoi nous faut-il l'enchâsser dans la Charte des droits et libertés?

Mme Elliott: Beaucoup de droits enchâssés dans la Charte des droits et libertés font également l'objet d'une législation parallèle. Je n'y vois pas aucun conflit.

M. Robinson (Etobicoke—Lakeshore): Je ne parle pas de conflit. Je me demande pourquoi il faudrait l'enchâsser dans la Charte des droits et libertés alors qu'on a déjà la Loi sur la protection des renseignements personnels. Je pourrais remettre en question certaines matières qui sont également prévues à la Charte des droits et libertés, alors que nous disposons d'autres lois ou d'autres protections.

Mme Elliott: La Loi sur la protection des renseignements personnels porte sur le droit, envisagé du point de vue fédéral, aux renseignements dont dispose le gouvernement. Elle ne

[Text]

this particular case, we do believe data that is stored on computer tapes, which is personal information, should be treated as property.

Mr. Robinson (Etobicoke—Lakeshore): In any event, in your view the concept of privacy and the notion of confidentiality should both be inscribed in the law.

Ms Elliott: In this particular brief?

Mr. Robinson (Etobicoke—Lakeshore): Yes.

Ms Elliott: Yes.

Mr. Robinson (Etobicoke—Lakeshore): Okay. You have also indicated, for violation of privacy, an action could be brought even without proof of damage. But if there are no damages, then what do you see as the penalty; or do you see any penalty provisions?

Ms Elliott: An action should be brought. Damage is rather difficult to define in terms of . . . Excuse me, could you refer me to the exact page you have there?

Mr. Robinson (Etobicoke—Lakeshore): On page 4, at the bottom of the first paragraph, you have a quote here; and that is what I wanted you to explain:

“An action for violation of privacy may be brought without proof of damage.”

I wanted you to explain that quote, and I was wondering if you were concerned about a penalty. If you are talking about penalties, then are you talking about criminal law per se?

Ms Elliott: This refers specifically to some legislation in Manitoba. Their provincial privacy legislation is quoted there simply to give a definition they are particularly using. We are not recommending this in the draft legislation having to do with computer theft or privacy. It is merely for illustrative purposes.

Mr. Robinson (Etobicoke—Lakeshore): All right. Going on, you indicate that, at the federal level, the legislation presently in being “is not broad enough to deal with computer theft”. Do you have any suggestions for provisions that would include this?

Ms Elliott: I think, by putting computer theft into the Criminal Code and defining computer software programs, data bases and so forth . . .

Mr. Robinson (Etobicoke—Lakeshore): Could you come up with a definition of computer theft or computer crimes per se that you think would suffice as an amendment?

Ms Elliott: No, no, we have no specific recommendations as to the phraseology.

Mr. Robinson (Etobicoke—Lakeshore): All right. On page 5 of your brief, you make the statement in the second paragraph that information is not defined as property. Do you have any definition of what it should be?

Ms Elliott: Of what property should be?

[Translation]

traite pas de renseignements personnels. Cependant, pour en revenir aux ordinateurs, et à ce cas-ci en particulier, nous croyons qu'il faudrait traiter comme propriété les données qui sont mises en mémoire sur les bandes d'ordinateur, c'est-à-dire les renseignements personnels.

M. Robinson (Etobicoke—Lakeshore): De toute façon, vous êtes d'avis que le concept de la vie privée et le caractère confidentiel devraient tous les deux être mentionnés dans la loi.

Mme Elliott: Pour ce mémoire en particulier?

M. Robinson (Etobicoke—Lakeshore): Oui.

Mme Elliott: Oui.

M. Robinson (Etobicoke—Lakeshore): Très bien. Vous avez également préconisé que toute violation de la vie privée donne lieu à poursuite, même sans preuve de préjudice. Toutefois, s'il n'y a pas de préjudice, que prévoyez-vous comme peine; ou avez-vous prévu des dispositions à ce sujet?

Mme Elliott: Il faudrait intenter une poursuite. Il est difficile de définir le préjudice selon . . . Excusez-moi, pouvez-vous me dire à quelle page vous en êtes?

M. Robinson (Etobicoke—Lakeshore): À la page 4, au bas du premier paragraphe, vous dites, et j'aimerais bien une explication à ce sujet:

On peut intenter une poursuite pour violation de la vie privée sans preuve de préjudice.

Je voulais que vous m'expliquiez ce passage et je me demandais si vous aviez songé à une peine. Si oui, s'agit-il là d'une proposition touchant le droit criminel?

Mme Elliott: Ce passage se rapporte spécifiquement à certaines lois du Manitoba. Nous avons cité la loi de cette province en matière de protection de la vie privée pour donner une définition dont on se sert dans cette province. Nous ne recommandons pas cette définition dans ce projet de loi qui a trait aux infractions relatives aux ordinateurs ou à la vie privée. Il ne s'agit que d'un exemple.

M. Robinson (Etobicoke—Lakeshore): Très bien. Vous poursuivez en disant qu'au niveau fédéral, la loi qui existe actuellement «n'est pas assez générale pour englober les infractions relatives aux ordinateurs». Avez-vous des suggestions pour des dispositions qui en tiendraient compte?

Mme Elliott: En prévoyant les infractions relatives aux ordinateurs dans le Code criminel et en définissant les logiciels, les bases de données et autres . . .

M. Robinson (Etobicoke—Lakeshore): Pouvez-vous nous donner une définition du vol ou des infractions relatives aux ordinateurs, qui suffirait, à votre avis, pour opérer une modification du Code criminel en conséquence?

Mme Elliott: Non, non, nous n'avons aucune recommandation spécifique concernant la phraseologie.

M. Robinson (Etobicoke—Lakeshore): Très bien. À la page 5 de votre mémoire, vous déclarez, au deuxième paragraphe, que les renseignements ne sont pas définis comme étant une propriété. Avez-vous une définition de ce qu'elle devrait être?

Mme Elliott: De ce que la propriété devrait être?

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): Yes, to include information.

Ms Elliott: I do not have that readily at hand, but I can certainly make it available to you. There is a draft.

Mr. Robinson (Etobicoke—Lakeshore): Fine, we would like to have that.

• 1610

And another matter I want to ask you about relates to page 8, where you say: "The issue here is not malice, but negligence."

I wonder if you could explain that a bit further. I am not quite sure what you are relating this to.

Ms Elliott: In some cases unauthorized access could be considered "malice"—that is, a desire to obtain information about authorization. In other cases, access may be making material inadvertently available.

Mr. Robinson (Etobicoke—Lakeshore): Are you saying that action should only be taken where there is malice but not where there is negligence?

Ms Elliott: As defined as theft?

Mr. Robinson (Etobicoke—Lakeshore): Well, I am thinking particularly of, say, the user who, with malice, maliciously obtains other information. Do you feel that is something which should be prosecuted? But if the user is just negligent in leaving the terminals on so that computer theft can take place, or leaves the code for somebody else to get at, would you consider that not to be actionable?

Ms Elliott: Perhaps that was not expressed clearly enough. It simply refers to the fact that more standards should be established in order to ensure that inadequately-protected systems are not legally authorized for access.

Mr. Robinson (Etobicoke—Lakeshore): On page 10 of your brief, in the second paragraph you say:

Electronic data processing and advanced telecommunications systems have removed most physical barriers to information collection, while our legal system has, in many cases, become too archaic to deal with these issues, . . .

In other words, you are just saying that it is not keeping up with the change in the technology. What do you recommend here? Are you recommending the specific changes now? Or do you recommend an ongoing look at the statutes in the Criminal Code to keep them updated as the technology advances?

Ms Elliott: One of the recommendations included in this particular brief is to strike a committee which would be made up of industry, consumers' government, and so forth—the idea being that they could come up with involuntary standards. Perhaps that would be the committee to look to for the

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Oui, pour inclure les renseignements.

Mme Elliott: Je ne l'ai pas au bout des doigts, mais je peux certainement vous la transmettre. Il y a un projet à ce sujet.

M. Robinson (Etobicoke—Lakeshore): Très bien, nous aimerions bien l'obtenir.

J'aimerais également vous poser une question au sujet d'une remarque que vous faites à la page 8, et je cite: «la question ici n'est pas la malice, mais la négligence..»

Vous serait-il possible de me fournir quelques explications supplémentaires là-dessus. Je ne vois pas très bien à quoi cela se rapporte.

Mme Elliott: Dans certains cas, l'accès non autorisé pourrait être considéré comme étant «un acte de malice» . . . autrement dit, cela correspond au désir d'obtenir des renseignements sans en avoir l'autorisation. Dans d'autres cas, l'accès met par inadvertance à la disposition d'autrui un certain nombre de données.

M. Robinson (Etobicoke—Lakeshore): Voulez-vous dire par là que des mesures ne devraient être prises que lorsqu'il y a malice, et non dans les cas où il s'agit purement de négligence?

Mme Elliott: Définie comme étant un vol?

M. Robinson (Etobicoke—Lakeshore): Je songe en particulier à l'utilisateur qui par malice obtient d'autres renseignements que ceux qu'il était censé se procurer. Pensez-vous que dans ce cas-là il faille tenter des poursuites? Mais si l'utilisateur est tout simplement négligent, s'il laisse le terminal ouvert, ce qui le met à la disposition d'un voleur, ou s'il laisse trainer le code, selon vous cela serait-il sujet à procès?

Mme Elliott: Peut-être que je ne me suis pas suffisamment bien exprimée. Je voulais tout simplement dire qu'il faudrait établir davantage de normes pour que l'accès aux systèmes mal protégés ne puisse être légalement autorisé.

M. Robinson (Etobicoke—Lakeshore): Vous dites dans le deuxième paragraphe de la page 10 de votre mémoire:

Le traitement électronique des données et les systèmes de télécommunication avancés ont éliminé la plupart des barrières physiques à la collecte de données, tandis que notre système juridique est dans bien des cas devenu trop archaïque pour pouvoir régler ces questions . . .

Autrement dit, selon vous, ce système ne suit pas l'évolution technologique. Que recommanderiez-vous? Recommandez-vous que l'on adopte dès maintenant un certain nombre de changements? ou plutôt qu'on examine régulièrement les statuts du Code criminel afin de les mettre à jour chaque fois qu'il y a des progrès technologiques?

Mme Elliott: L'une des recommandations formulée dans notre mémoire vise la création d'un Comité qui serait composé de représentants de l'industrie, des consommateurs, du gouvernement etc., . . . l'idée étant que ces personnes pourraient établir ensemble des normes obligatoires. Et ce même

[Text]

provision of recommendations and the monitoring of these kinds of changes.

Mr. Robinson (Etobicoke—Lakeshore): An off-shoot committee from the consumer group that you represent, the Consumers' Association of Canada?

Ms Elliott: The Consumers' Association is always ready to participate in these kinds of activity.

Mr. Robinson (Etobicoke—Lakeshore): On page 12, you have an inserted paragraph which I guess is from R. Bloom . . .

Ms Elliott: Yes.

Mr. Robinson (Etobicoke—Lakeshore): —and the last sentence of that says:

The risk of being caught, let alone prosecuted and convicted, is very low.

I suppose that is really the key to the whole thing. How do you obviate risk? Obviously, no one commits a crime with the expectation of being caught. So how do you bring it home to the people who are likely to perpetrate theft or to trespass, whatever it is in computer crime, that they are going to be caught? Would this be done through an elaborate system of security? In what way do you see this being done? How do we lessen the risk?

Ms Elliott: On one side of the issue we, as I say, ensure there is adequate protection against access; that it be constantly updated and upgraded with the idea that property is important, and it is an invasion of privacy to obtain it. On the other hand, we assume there are suitable modes to prosecute. In the past, in fact, even if your were "caught", there has not been adequate legislation to provide any kind of redress.

Mr. Robinson (Etobicoke—Lakeshore): Have you or your organization given any consideration to a code of ethics for users, practisers, involved in the computer industry, data processing, and so on?

Ms Elliott: Not in those terms, no. When we suggested a committee being formed, made up of wide representation, we are effectively suggesting that there should be some standards when it comes to providing security. We believe it has to be dealt with on both sides.

Mr. Robinson (Etobicoke—Lakeshore): Have you written out what you consider to be the kinds of standards, guidelines or regulations, which you feel would be most effective?

Ms Elliott: No.

Mr. Robinson (Etobicoke—Lakeshore): Do you have that information, or are you considering providing such?

• 1615

Ms Elliott: At present, I could not answer that because our association has not covered this material in detail.

[Translation]

comité pourrait peut-être également être chargé de formuler des recommandations et de contrôler l'exécution des changements.

M. Robinson (Etobicoke—Lakeshore): Il s'agirait d'un comité émanant du groupe de consommateurs que vous représentez, c'est-à-dire l'Association canadienne des consommateurs?

Mme Elliott: L'Association canadienne des consommateurs est toujours prête à participer à ce genre d'activités.

M. Robinson (Etobicoke—Lakeshore): À la page 12, vous avez inséré un paragraphe qui est tiré du rapport de R. Bloom . . .

Mme Elliott: Oui.

M. Robinson (Etobicoke—Lakeshore): . . . et voici ce que dit la dernière phrase:

Le risque de se faire prendre, sans parler de celui d'être poursuivi et inculpé, est très faible.

Je suppose que c'est là la clef de toute l'affaire. Comment prévenir le risque? Il est évident que personne ne commet un crime s'il s'attend à se faire prendre. Alors comment faire comprendre aux personnes qui seraient tentées de violer des systèmes électroniques ou de commettre d'autres crimes relativement aux ordinateurs, qu'elles se feraient prendre? Cela se ferait-il dans le cadre d'un système de sécurité complexe? Selon vous, comment cela pourrait-il se faire? Que peut-on faire pour diminuer le risque?

Mme Elliott: Tout d'abord, comme je l'ai déjà dit, il faut assurer une protection adéquate contre l'accès; et cette protection doit sans cesse être mise à jour en soulignant que la propriété est importante et que l'obtention d'éléments de cette propriété constitue une atteinte à un droit. D'autre part, nous prenons pour acquis qu'il existe des poursuites adéquates. Par le passé, même si vous vous faisiez prendre, la loi ne prévoyait pas de solutions satisfaisantes.

M. Robinson (Etobicoke—Lakeshore): Avez-vous, vous ou votre organisme, examiné la question d'un code d'éthique pour les utilisateurs et les autres personnes qui travaillent dans le domaine de l'informatique, du traitement des données, etc.?

Mme Elliott: Non, pas dans ces termes-là. Lorsque nous proposons la création d'un comité, comité qui serait représentatif de tous les secteurs de la société, ce que nous proposons en fait, c'est qu'il y ait des normes en matière de sécurité. Nous pensons qu'il faut s'attaquer au problème des deux côtés.

M. Robinson (Etobicoke—Lakeshore): Avez-vous rédigé des normes, des lignes directrices ou des règlements qui seraient, selon vous, les plus efficaces?

Mme Elliott: Non.

M. Robinson (Etobicoke—Lakeshore): Disposez-vous de renseignements à ce sujet, ou prévoyez-vous nous en fournir?

Mme Elliott: Je ne puis répondre tout de suite à cette question, car notre association n'a pas encore fait d'étude approfondie du problème.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): In your recommendation (b) on page 17 of your brief, you indicate that you:

recognize the need for the establishment of standards for the confidentiality and security of client data . . .

-and so on, and I just assumed that you would be thinking of a code of ethics or a set of standards, regulations and so on, which might be useful.

Ms Elliott: I indicated that we would see that voluntary setting of, and adherence to, standards plus a mechanism for monitoring is our recommendation to the committee.

Mr. Robinson (Etobicoke—Lakeshore): Yes. Thank you very much, Madam Chairman.

Le président: Merci, monsieur Robinson.

Monsieur Beatty.

Mr. Beatty: Thank you, Madam Chairman. Let me start by thanking the representatives of the CAC for a very useful and enlightening brief, and a very helpful presentation. Mr. Robinson covered a number of the points that I had marked, but I wondering whether I may ask you about two or three issues.

The first is the question of copyright, which you do not deal with in your brief. One of the elements of computer crime that is of concern to the committee is the issue of copyright and whether a computer's software and data should be copyrightable. Have you taken any position on that and, if so, what would that be?

Ms Elliott: I am afraid we have not as yet.

Mr. Beatty: Could we then go to the point (b) on page 17, part of which Mr. Robinson quoted a minute ago. I refer to the question of recognizing the need for the establishment of standards for the confidentiality and security of client data for both privately- and publicly-controlled personal data systems and developing a mechanism for monitoring and compliance. To an extent, I suppose that is similar to Professor David Flaherty's recommendations to the committee. Most recommendations we have had to date have not included imposing some external standards on the holders of information to ensure that they maintain adequate security, although one can recognize the importance of it.

Like Mr. Robinson's, my concern is essentially how you would do that. What standards would you see applying? How would they be set? Would an individual have a right to sue a company? Take, for example, one of the insurance companies in London, or the University of Western Ontario. If the data bank containing information about individuals in either case was violated, should the individual have the right to sue the institution on the grounds that information about the individual had been given out without his consent?

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Vous dites dans votre recommandation (b) à la page 17:

reconnaître le besoin d'établir des normes pour le caractère confidentiel et la sécurité des données sur les clients . . .

. . . etc., et j'en ai déduit que vous songiez à un code d'éthique ou à un ensemble de normes ou de règlements qui pourraient être utiles.

Mme Elliott: Je vous ai expliqué que nous recommanderions au Comité d'établir des normes ainsi qu'un mécanisme de contrôle et de veiller à leur application.

M. Robinson (Etobicoke—Lakeshore): Oui. Merci beaucoup, madame le président.

The Chairman: Thank you, Mr. Robinson.

Mr. Beatty.

M. Beatty: Merci, madame le président. J'aimerais tout d'abord remercier les représentants de l'ACC pour leur mémoire que j'ai trouvé très utile et très révélateur. M. Robinson a soulevé un certain nombre de points qui m'intéressaient, mais j'aimerais vous poser deux ou trois questions.

La première concerne le droit d'auteur, dont vous ne faites pas état dans votre mémoire. L'un des éléments des crimes relatifs aux ordinateurs qui intéressent le Comité, c'est la question du droit d'auteur. Nous nous demandons si le logiciel et les données informatiques devraient pouvoir être couverts par le droit d'auteur. Avez-vous pris position là-dessus et, dans l'affirmative, quelle serait-elle?

Mme Elliott: Malheureusement, nous n'avons pas encore pris position là-dessus.

M. Beatty: Je passerai donc au point (b) à la page 17, dont M. Robinson a cité une partie. Je me réfère à la question de reconnaître le besoin d'établir des normes pour protéger le caractère confidentiel et la sécurité des données sur les clients tant pour les systèmes privés que pour les systèmes de données personnelles qui sont gérés par des organismes publics, et à la question de l'élaboration d'un mécanisme de contrôle et de vérification de l'application. Je suppose que cela rejoint dans une certaine mesure les recommandations qui ont été soumises au Comité par le professeur David Flaherty. La plupart des recommandations que nous avons entendues à ce jour ne comprenaient pas l'imposition de normes externes sur les détenteurs de données afin d'assurer que ces derniers maintiennent des systèmes de sécurité adéquats, même si d'aucuns ont reconnu l'importance de cela.

Je me demande, tout comme M. Robinson, comment vous feriez cela. Selon vous, quelles normes s'appliqueraient? Comment seraient-elles établies? Un particulier aurait-il la possibilité d'intenter des poursuites contre une société? Prenez, par exemple, une société d'assurance à London, ou la *University of Western Ontario*. Si la banque de données d'une de ces sociétés ou de l'université, banque de données qui contiendraient des renseignements au sujet de certaines personnes, était violée, un particulier aurait-il le droit de poursuivre l'institution pour cause de divulgation de renseignements à son sujet sans son consentement?

[Text]

Ms Elliott: I believe that opportunity exists currently under common law. The chances of obtaining redress are not as great, but there have been instances where that has occurred. I can forward to you the specific case or the outline of the case within it.

As to the specific issue of which standards should be applied, first, I think we were concerned that the kind of data held, and the size and sensitivity of the data, should require some flexibility in standard-setting, right off the top. That was what encouraged us to make this kind of voluntary standard setting. I do not think I have answered your question though.

Mr. Beatty: I have essentially two concerns. One is I think that Professor Flaherty was somewhat stretching the mandate of the committee in drawing computer crime over privacy quite as broadly as he did. There is certainly a strong element of the privacy issue involved in computer crime. One is able to violate a data base which has personal information about an individual, and there is great potential there for violation of one's privacy, but I am not sure that a bill dealing with computer crime is the best way to enact standards to protect people's privacy.

For example, take theft. If I were to break into your house and steal materials which belong to you, I might be invading your privacy at the same time, but one would not seek to establish standards for privacy under the guise of legislation dealing with theft as such.

Ms Elliott: We are really not talking about standards to secure privacy, but standards to secure personal information held in computers. The consumer issue is that it is essentially one and the same, I am not certain that you can draw such a strict parallel.

Mr. Beatty: The point that I am trying to make is that the mandate of the subcommittee is relatively narrow: we are to look at computer crime as such, and what problems there are in the law as it stands today. The chief concern of the CAC and, also, of Professor Flaherty was in the issue of privacy per se.

• 1620

There is an area there where the two concerns intersect, but I am not sure that legislation dealing with computer crime is in itself adequate to deal with the privacy issue and I suspect that what we may have to do as one of our recommendations is to suggest that more study be given to the privacy issue and whether or not some privacy legislation should be passed dealing with privacy as such, which might extend the principles which currently exist . . .

[Translation]

Mme Elliott: Je pense que le droit commun prévoit déjà cette possibilité. Les chances d'obtenir réparation ne sont pas aussi bonnes, mais je connais des cas où cela s'est fait. Je pourrais vous fournir davantage de précisions au sujet du cas auquel je songe.

Pour ce qui est de la question de savoir quelles normes devraient être imposées, je pense qu'il convient de préciser que le genre de données dont il s'agit, ainsi que leur envergure et leur importance, devraient exiger une certaine souplesse pour ce qui est de l'établissement de ces normes, et ce, dès le départ. C'est ce qui nous a encouragés à opter pour une formule d'établissement de normes facultatives. Mais je ne pense pas avoir répondu à votre question.

M. Beatty: En gros, deux choses me préoccupent. Tout d'abord, je pense que le professeur Flaherty a quelque peu déformé le mandat du Comité en définissant aussi largement qu'il l'a fait l'aspect privé ou confidentiel des données qui peuvent faire l'objet de crimes relatifs aux ordinateurs. L'aspect privé de certaines données est certes un élément important du problème. Il est possible de violer une base de données qui contient des renseignements très personnels au sujet de quelqu'un, et donc d'empiéter sur sa vie privée. Mais je ne suis pas certain que la rédaction d'un projet de loi au sujet des crimes relatifs aux ordinateurs serait le meilleur moyen d'imposer des normes visant à protéger la vie privée des gens.

Prenez le vol, par exemple. Si je pénétrais dans votre maison et si je volais un certain nombre de choses qui vous appartiennent, je pourrais en même temps être en train de violer votre vie privée, mais on n'essaierait pas d'établir des normes en matière de vie privée dans le contexte d'une loi qui traite du vol en tant que tel.

Mme Elliott: Nous ne parlions en fait pas de normes pour garantir le respect de la vie privée, mais plutôt de normes pour garantir la protection de renseignements personnels contenus dans des ordinateurs. Le problème, c'est que du point de vue des consommateurs, cela revient plus ou moins à la même chose, et je ne suis pas certain qu'il soit possible de dresser un parallèle.

M. Beatty: Ce que j'essaie d'expliquer, c'est que le mandat du sous-comité est assez étroit: nous devons étudier les crimes relatifs aux ordinateurs en tant que tels, et les problèmes qui existent dans la loi actuelle. Or, ce qui préoccupe surtout l'ACC et le professeur Flaherty, c'est la question de la vie privée en tant que telle.

Il y a là un domaine dans lequel les deux problèmes se recoupent, mais je ne pense pas qu'un projet de loi sur les crimes liés à l'informatique suffise en soi à assurer le respect du droit à la vie privée; à titre de recommandation, nous pourrions peut-être proposer de faire davantage de recherches sur le problème du droit à la vie privée pour voir s'il serait nécessaire d'adopter une loi spécifique à ce sujet, qui pourrait, par exemple, élargir les principes déjà en vigueur . . .

[Texte]

Ms Elliott: CAC would agree with you, and our method of approaching the issue of privacy has really been three-pronged. Computer theft is certainly one aspect of it as it interfaces, but we are also recommending privacy legislation per se. In this particular case, we are dealing strictly with the personal information, health and the privacy interface.

Mr. Beatty: Sticking, then, to the more narrow concern of where computer theft occurs... and I think both of us can agree that there may be a problem, that an institution may be negligent in terms of its own security—can you just run past me again the procedures that you would see being put in place by the government to require that institutions maintain adequate data security? It seems to me that the degree of security is going to vary from case to case. I would be far less worried if the subscription list of *The Financial Post* were stolen than if my tax records or my medical file were stolen, and the degree of security on those files might vary depending on their content. How would you establish those standards, how would government enforce it, and what sort of mechanism would you see for achieving the goal that you and I both agree would be desirable?

Ms Elliott: Initially, given our interest in personal information and the privacy aspect of it, we would define information, the kind of personal information, and the ability and access of the system, the type of system—how interactive it is, how many users are on it—and review each broad sub-set of both the equipment and the information available to establish some sort of benchmark of standards. We are not recommending that the government legislate or enforce; we are suggesting that voluntary standards at present certainly should be tried given the wide range of different systems and information held. We are suggesting that there should be a mechanism for monitoring for clients. More specifically, it has been suggested that auditors or EDP auditors be given the task of reviewing or at least reporting on the kind of systems that have been put in place to protect or to restrict access and so forth.

Mr. Beatty: You would not have any sanctions that could be taken against an institution which did not meet the voluntary standards?

Ms Elliott: At present, no.

Mr. Beatty: Would you be satisfied with a recommendation from the committee which would be essentially that the government consider the creation of a study group in conjunction with industry, consumers' groups and other interested groups and individuals to look at the question of EDP security and to make recommendations for the development of standards which could be incorporated by institutions to protect privacy?

Ms Elliott: We would be happy to see that step taken. We are recommending that it go one further, that a committee be struck as soon as possible to set those standards. That it would be spearheaded by the government, or at least established by

[Traduction]

Mme Elliott: L'ACC est d'accord avec vous et, en fait, notre approche vis-à-vis de ce problème comporte trois volets. Le vol est sans doute un aspect du problème, mais nous recommandons également l'adoption d'une loi sur le respect de la vie privée. Il s'agirait alors strictement des renseignements personnels, qui comprennent les renseignements médicaux et les renseignements d'ordre intime.

M. Beatty: Limitons-nous alors au problème du vol dans le domaine de l'informatique. Je crois que vous reconnaissez avec nous qu'à cet égard il se peut qu'un organisme soit négligent sur le plan de sa propre sécurité; toutefois, j'aimerais que vous répétiez les procédures que vous recommandez au gouvernement d'instaurer pour obliger ces organismes à prendre les précautions suffisantes. À mon avis, le degré de sécurité nécessaire variera d'un cas à l'autre, car, en ce qui me concerne, le vol de la liste des abonnés du *Financial Post* serait certainement moins grave que le vol de mes déclarations d'impôt ou de mes dossiers médicaux. En conséquence, les précautions que le gouvernement pourrait exiger quant à la sécurité de ces dossiers varieraient sans doute en fonction de leur contenu. À votre avis, comment pourrait-on définir ces normes et comment le gouvernement pourrait-il les faire appliquer? Par quel mécanisme pensez-vous que nous pourrions atteindre cet objectif que vous et moi jugeons souhaitable?

Mme Elliott: Au départ, étant donné que nous nous intéressons de très près aux renseignements personnels et à leur caractère confidentiel, nous pensons qu'il faudrait définir ces renseignements personnels ainsi que les conditions dans lesquelles on peut avoir accès au système, c'est-à-dire quels sont ces usagers, et cetera. On pourrait ensuite établir une sorte de barème en fonction de chaque sous-catégorie générale à la fois pour le support et pour les renseignements. Nous ne recommandons pas que le gouvernement adopte des lois à ce sujet; nous estimons qu'on devrait d'abord essayer de voir ce que donnent les normes actuelles avec une vaste gamme de systèmes et de renseignements différents. Nous estimons qu'il devrait y avoir un mécanisme permettant de contrôler les clients. Plus précisément, il a été suggéré que les vérificateurs du PED soient chargés de faire un rapport sur les systèmes qui ont été mis en place afin de les protéger ou d'en restreindre les conditions d'accès.

M. Beatty: Vous ne proposez pas l'adoption de sanctions contre un organisme qui n'adopterait pas ces normes?

Mme Elliott: Pas pour l'instant.

M. Beatty: Accepteriez-vous une recommandation du Comité demandant en substance au gouvernement d'envisager la constitution d'un groupe d'étude en collaboration avec l'industrie, les groupes de consommateurs et tous les autres groupes et particuliers intéressés, afin d'étudier la question de la sécurité du TED et afin de faire des recommandations sur les normes que devraient adopter les différents organismes pour protéger le droit à la vie privée des citoyens?

Mme Elliott: Nous serions tout à fait d'accord là-dessus. Nous recommandons même d'aller plus loin, à savoir qu'un comité soit constitué le plus vite possible par le gouvernement pour établir ces normes. Donc, il est bien évident que nous

[Text]

the government, is assumed. Yes, we would like to see action in that area. We are not recommending legislation at present.

Mr. Beatty: One area that you did not touch on in your brief—Mr. Robinson alluded to it again—was the question of a code of ethics. One of the recommendations being made by various groups before us was that in institutions that teach students about computer programming and other aspects of computer science there be courses on computer ethics in the same way business schools give courses on business ethics or medical schools on medical ethics and so on. Would you feel that this would be a useful recommendation for the committee to make as a possible means of sensitizing people who will be working with EDP systems to privacy issues, among others?

Ms Elliott: It seems like a worthwhile suggestion. I think my review of the literature indicates a considerable interest and sensitivity in the industry at the moment. To draw to their attention not just the property end of computer theft but also the privacy end would be very worthwhile.

• 1625

Mr. Beatty: The final area I had a note about was the recognition of the right or the need to entrench the right to individual privacy in the Charter of Rights and Freedoms. It is an area where I am ambivalent. The issue of privacy has been a key issue to me during much of the past 10 years, particularly as it relates to the social insurance number, and I had responsibility in the Clark government for drawing up the provisions of the freedom of information-privacy legislation dealing with privacy in the social insurance number. I strongly support legislation to protect individual privacy, and indeed when I was on the committee on the Constitution I believe some of my colleagues put a motion to entrench the right to privacy in the charter. I am somewhat equivocal on that, though, and hesitant, in that without an adequate definition of what "privacy" means one could extend the concept very, very broadly.

For example, I believe in the United States, unless I am mistaken, the issue of privacy was extended into the issue of abortion. It seems to me that while it is entirely appropriate for governments to legislate on abortion, they should do so knowing what they are legislating on and not do so unconsciously by writing vague provisions in the law which subsequently get interpreted by the courts in a way that was not anticipated by the legislature at the time.

What thought have you given to the potential problems that could be posed in incorporating a concept as vague as privacy, where it means different things to different people in the Charter of Rights, and having it subsequently interpreted by the courts?

Ms Elliott: The impetus for making that recommendation really came from review of some of the case examples on privacy that we ran across in our research. It appeared that

[Translation]

aimerions que des mesures soient prises dans ce domaine, mais nous ne recommandons pas pour l'instant l'adoption d'une loi.

M. Beatty: Au cours de votre exposé, vous n'avez pas parlé, et M. Robinson y a fait allusion, d'un code de déontologie. Plusieurs des témoins qui ont comparu devant nous nous ont recommandé que les établissements qui dispensent des cours d'informatique incluent également des cours sur la déontologie en matière d'informatique, de la même façon que les écoles de commerce dispensent des cours sur la déontologie commerciale, et les facultés de médecine, des cours sur la déontologie médicale. Pensez-vous que notre comité devrait faire cette recommandation, dans le but de sensibiliser les futurs techniciens et programmeurs au problème du droit à la vie privée des citoyens, entre autres?

Mme Elliott: Cette suggestion me paraît fort valable. D'après ce que j'ai pu lire, l'industrie s'intéresse actuellement beaucoup à cette question. Il me semble donc qu'il serait tout à fait valable d'attirer leur attention, non seulement sur les conséquences concrètes du vol dans le domaine de l'informatique, mais également sur ses conséquences au niveau du droit à la vie privée du simple citoyen.

M. Beatty: La dernière question que je voulais aborder avec vous concerne la reconnaissance ou la consécration du droit à la vie privée dans la Charte des droits et des libertés. Je vous avoue que je suis un peu partagé sur cette question. Certes, le droit à la vie privée est une question qui m'intéresse énormément depuis dix ans, surtout pour ce qui est du numéro d'assurance social; de plus, sous le gouvernement Clark, j'ai été chargé de préparer les dispositions du projet de loi sur la liberté de l'information et la protection des renseignements personnels, ainsi que celles concernant le numéro d'assurance social. J'appuie fermement le projet de loi destiné à protéger le droit à la vie privée, et en fait, lorsque j'étais membre du Comité sur la Constitution, je crois que l'un de mes collègues a proposé une motion destinée à consacrer dans la charte le droit à la vie privée. Cependant, je suis un peu hésitant, car je crains qu'en l'absence d'une définition adéquate de l'expression «droit à la vie privée», on ne lui donne une interprétation très, très générale.

Par exemple, si je ne me trompe, on est allé à invoquer le droit à la vie privée aux États-Unis au sujet de l'avortement. Certes, les gouvernements sont tous à fait habilités à légiférer en matière d'avortement, mais ils devraient le faire en sachant parfaitement ce sur quoi ils légifèrent, et non pas en proposant des dispositions libellées de façon vague qui seront par la suite interprétées par les tribunaux d'une manière non prévue par les législateurs.

Avez-vous réfléchi aux problèmes éventuels que risquerait de poser la consécration dans la charte d'un concept aussi vague que le droit à la vie privée, dont la signification varie d'une personne à l'autre, et dont l'interprétation peut également varier d'un tribunal à l'autre?

Mme Elliott: Nous avons préparé cette recommandation à la suite d'une étude de certains des cas que nous avons eu l'occasion de rencontrer au cours de nos recherches, et je parle

[Texte]

while the right of privacy was not really affirmed in tort law or in the courts, when an issue came up against specific legislation such as the Canada Evidence Act or the Income Tax Act, the courts did act, where they had the opportunity, to respect or to deal with the issue of invasion of privacy. We also felt in our own experience with consumers and their response that it was generally viewed to be a right that people had. They did not understand that per se it was not a right. Therefore the recommendation to entrench it in the charter came from that action.

As for defining individual privacy, which is really the key issue here, I do not have any specific recommendations on that at the moment. But I acknowledge your . . .

Mr. Beatty: You anticipated what was going to be my next question: that is, whether you could give a succinct definition of what you mean when you use the word; because I think "privacy" is really a code word we use to mean much more than the traditional dictionary definition of the word. The simplest definition is the right to be left alone. What you and I mean when we use the term today in terms of legislation is much broader than that. For example, the privacy legislation that was passed by Parliament and may be proclaimed on July 1 includes the concept of the right of the individual to know what information is held about them, to have access to that information, to challenge the information if it is incorrect. All of that goes well beyond any dictionary definition of what "privacy" means.

Ms Elliott: I would define it shortly as unauthorized access to personal information.

Mr. Beatty: Okay. Let us get down to hard cases, then. The easiest way, I suppose, for any of us to look at the privacy issue, and the way I have traditionally looked at it, is almost on the basis of property: that information about myself is property which I own and which another should not control without my informed consent. We often surrender rights to information about ourselves and do so willingly to participate in a program or to obtain credit or what have you. That is good as far as it goes; but by watching you sitting across from me at the table today, I am able to gain personal information about you that theoretically I could put into a file about you. I am not sure we have press here today who have the right to write about what you have said, the way in which you said it, the way in which you appeared before the committee. All of this would relate to your person as an individual.

• 1630

I am not sure that you or that I would claim the right to prevent them from reporting that information. So we recognize that even with information relating to ourselves as a person, we do not have absolute control over it. It seems to me that that definition of privacy that you would offer, quickly when you get down to hard cases, becomes inapplicable.

[Traduction]

toujours du droit à la vie privée. Apparemment, même si le droit à la vie privée n'était pas véritablement reconnu par le droit civil ou par les tribunaux, lorsqu'un cas de ce genre se présentait au sujet d'une loi spécifique comme la Loi sur la preuve au Canada ou la Loi sur l'impôt sur le revenu, les tribunaux se sont efforcés, lorsque cela était possible, de respecter ou tout au moins d'étudier le problème de l'intrusion dans la vie privée. Au cours de notre expérience auprès des consommateurs, nous avons constaté que c'était un droit généralement accepté. Ils ne comprenaient pas pourquoi, en soi, ce n'était pas un droit. C'est pour cela que nous recommandons de consacrer ce droit dans la Charte des droits.

Quant à la définition du droit à la vie privée, c'est évidemment le problème fondamental, mais je n'ai pas de recommandation particulière à vous faire pour le moment. Je reconnais cependant que votre . . .

M. Beatty: Vous devinez sans doute quelle va être ma question suivante: pourriez-vous me donner une définition succincte de ce que vous voulez dire lorsque vous employez cette expression? J'ai l'impression que c'est un cliché auquel nous donnons une signification beaucoup plus vaste que la définition traditionnelle du dictionnaire. En termes simples, c'est le droit d'exiger qu'on vous laisse tranquille. Cependant, lorsque vous et moi employons cette expression, aujourd'hui, dans le cadre de la loi, le sens est beaucoup plus vaste. Par exemple, la Loi sur la protection des renseignements personnels, qui a été adoptée par le Parlement et qui sera peut-être promulguée le 1^{er} juillet, inclut le droit de l'individu de connaître quels renseignements on détient à son sujet, d'avoir accès à ces renseignements et de les contester s'ils sont erronés. Tout cela va bien plus loin que la simple définition du dictionnaire.

Mme Elliott: En quelques mots, je définirai cette expression comme l'accès illégitime à des renseignements personnels.

M. Beatty: Bien. Passons maintenant à des situations plus délicates. La façon la plus simple d'aborder les problèmes du droit à la vie privée est de partir de la notion de propriété: quels renseignements me concernant m'appartiennent et ne devraient donc pas relever du contrôle d'une autre personne sans mon consentement, en connaissance de cause. Nous renonçons souvent à nos droits en acceptant de donner des renseignements sur nous-mêmes afin de pouvoir participer à un programme, de pouvoir obtenir du crédit, etc.. Jusque-là, parfait; vous êtes assise en face de moi, et en théorie ce que j'apprends sur vous, je pourrais le consigner dans un dossier. Je ne sais pas s'il y a des journalistes ici, qui ont le droit de rédiger un article sur ce que vous avez dit, sur la façon dont vous l'avez dit et sur la façon dont vous avez témoigné devant notre comité. Tout cela fait partie de votre vie privée personnelle.

Je ne suis pas sûr que vous ou moi pourrions réclamer le droit de les empêcher de transmettre cette information. Nous reconnaissons donc que même si cette information nous vise personnellement comme individus, nous n'avons pas un contrôle absolu sur elle. Il me semble que cette définition que

[Text]

Ms Elliott: I agree it is a difficult proposition, but I do not believe it is impossible. I think the general understanding of most consumers, most citizens, that they do have a right to privacy should make our efforts to define it doubly important.

Mr. Beatty: It is similar I suppose to the American concept of the pursuit of happiness. I am not entirely sure what that means either, but it seems to me that perhaps as opposed to enshrining the term "privacy" in legislation, what we should be doing is enshrining the various characteristics that we feel are important: that of access to information that is held about us; the right to challenge information that is false; the right to withhold information from institutions if it is not directly relevant and necessary to them; the right to demand that information be purged after it has outlived its usefulness. All of these would be deemed, I think, to be characteristics of privacy, and they might be much more susceptible to legislation than the term itself would be, and it might make perhaps a cleaner way of dealing with the issue than to put the concept as such on the line.

Ms Elliott: You are really answering the list of questions we are suggesting consumers should ask about personal information—Do you need to know? Why do you need to know? What are you going to do to keep it secure and up to date, and so forth?—defining privacy in those ways. We give a tool to consumers to find out just how much of their privacy is being invaded when they ask those questions. So I would agree with you that those are aspects of defining the word.

Mr. Beatty: Even in those terms it gets very difficult. Do I need to know the fact that you wear glasses? I do not need to know it, but I have access to the information. At this point I think Parliament would have great difficulty enshrining in law these principles and extending them broadly into the private sector.

The intention of the government, both at the time that Part IV of the Human Rights Act was passed, also at the time the Clark government drew up legislation on privacy and the time Parliament passed the freedom of information and privacy bill, was to try to develop those concepts on the strength of experience within government and then to move from there into the private sector. We have had very little experience in government so far. The act has not been proclaimed as yet, and I guess my concern is that we may need some more experience at the federal level with the definition of these concepts and how these rights are to be exercised before we can extend them into the private sector on a broad basis.

Now obviously already there is legislation in the Bank Act which provides for security standards on information. There are provisions in credit reporting acts of various provinces which deal with it and, by and large, governments to date have taken an ad hoc approach. My suspicion is that no matter how desirable I may feel that privacy legislation is, and I strongly

[Translation]

vous donneriez de la vie privée devient rapidement inapplicable en pratique.

Mme Elliott: Je reconnais que c'est difficile, mais je ne pense pas que ce soit impossible. A mon avis, comme la plupart des consommateurs, des citoyens pensent généralement qu'ils ont droit à la vie privée, cela devrait rendre doublement importants nos efforts pour la définir.

M. Beatty: Je présume que c'est semblable au concept américain de la poursuite du bonheur. J'ignore ce que cela veut dire exactement, mais il me semble qu'au lieu d'enchâsser le terme «vie privée» dans la loi, nous devrions peut-être mentionner certains de ses aspects, nous croyons être importants: il y a l'accès à l'information que l'on a pour nous, le droit de contester des renseignements qui sont faux, le droit de ne pas divulguer des informations à certaines institutions si elles ne sont pas directement pertinentes ou nécessaires à leur activité le droit de demander que les renseignements soient éliminés lorsqu'ils ne sont plus utiles. Il me semble que toutes ces choses sont des aspects de la vie privée et qu'elles sont plus susceptibles de faire l'objet d'un projet de loi que le terme lui-même, et ce serait peut-être une façon plus claire de traiter de ces questions que de viser le concept comme tel.

Mme Elliott: En fait, vous répondez à la liste de questions que nous suggérons aux consommateurs de poser en ce qui concerne l'information personnelle... Est-il nécessaire que vous sachiez? Pourquoi avez-vous besoin de le savoir? Que ferez-vous pour garantir la sécurité des renseignements et leur mise à jour, et ainsi de suite? ... C'est une manière de définir la vie privée. Nous donnons aux consommateurs un outil pour leur permettre de savoir, en posant ces questions, jusqu'à quel point on empiète sur leur vie privée. Je suis donc d'accord avec vous, ce sont des façons de définir ce terme.

M. Beatty: Même en ces termes, cela devient très difficile. Ai-je besoin de savoir que vous portez des lunettes? Je n'ai pas besoin de le savoir, mais j'ai accès à cette information. En ce sens, je pense qu'il serait très difficile pour le Parlement d'enchâsser ces principes sous forme de loi et de les appliquer de façon générale au secteur privé.

L'intention du gouvernement, au moment où l'on a adopté la Partie IV de la Loi sur les droits de la personne et aussi au moment où le gouvernement Clark a rédigé une loi sur la vie privée et où le Parlement a adopté la Loi sur le libre accès à l'information et sur la vie privée, c'était d'essayer d'élaborer ces concepts à partir de l'expérience acquise au sein du gouvernement, et de là, de les appliquer au secteur privé. Jusqu'ici, nous avons très peu d'expérience au gouvernement. La Loi n'a pas encore été proclamée et ce qui me préoccupe, c'est que nous avons besoin d'un peu plus d'expérience au niveau fédéral concernant la définition de ces concepts et la façon dont ces droits sont exercés, avant de pouvoir les étendre au secteur privé de façon générale.

Il est évident qu'il y a déjà une disposition de la Loi sur les banques qui prévoit des normes de sécurité sur l'information. Il y a des dispositions dans les lois provinciales sur la divulgation concernant la solvabilité des gens qui traitent de cela et, de façon générale, jusqu'ici les gouvernements ont adopté une approche ad hoc. Aussi souhaitable que soit cette législation—

[Texte]

support it at the federal level, we may need more time to see how it works at the federal level before attempting to extend the principles into the private sector at this point.

Ms Elliott: Do you not feel that the experience in some of the provincial jurisdictions would be helpful?

Mr. Beatty: I certainly feel it would be helpful, but I am not sure that it is satisfactory at this point. I think that is my difficulty. Even if you look at school boards and the information they have about students, employee records, medical records, what right of access should an individual have to his medical record if information about the fact that he has a terminal disease could in fact be damaging to his condition in the opinion of his doctor?

Ms Elliott: According to the Credit Reporting Act, although the doctor may provide that to the credit agency with the approval of the subject, the subject may not have access to that when he goes into check his records.

• 1635

Mr. Beatty: But what I am saying is, at this point I am not sure even with medical records that we are in a position that we could write a statute on privacy in medical records where we would feel entirely comfortable that we understood the implications of what we were doing. And that is just one small aspect of the information that is held on an individual. If you look upon the issue in a much broader way it becomes mind-boggling and I just do not think we have the experience at this point that we can go that far. I think it will take some time before we do and perhaps what we should be doing is, where it is clear there is a need, we could start dealing in nibbles to an extent. We can deal with it on the computer crime aspect and say that it is clear that if someone gains unauthorized access to your personal records because of a loophole in the Criminal Code, then there is a very real threat to your privacy and that should be closed off now. And there is no strong argument I have heard made against that before the committee.

There are a number of other areas like that, perhaps, where we can act on an ad hoc basis. My only hesitation is whether or not we can have one privacy bill for the private sector at this point and whether it is practicable for us to be doing that.

Ms Elliott: I would assume, in the case of computer theft and development of standards and development of monitoring systems, you would obtain a great deal of information regarding privacy, just through that methodology alone, by assigning essentially the importance and relevance of the systems and personal data.

Mr. Beatty: Yes. And I think your recommendation for a study is a very useful one that can help to generate that body of information to work from.

Well, thank you very much for a very helpful brief and for your elaboration. I appreciate it very much.

[Traduction]

et j'appuie fortement l'application d'une telle loi au niveau fédéral—je crains que nous ayons besoin de plus de temps pour voir comment cela fonctionne au niveau fédéral avant d'essayer d'étendre ces principes au secteur privé.

Mme Elliott: Ne croyez-vous pas que l'expérience de certaines provinces pourrait être utile?

M. Beatty: Je pense certainement que cela pourrait être utile, mais j'ignore si cela sera suffisant pour l'instant. Je pense que c'est là le problème. Même si l'on prend les commissions scolaires, elles ont des renseignements au sujet des étudiants, des dossiers sur les employés, des dossiers médicaux, quel droit d'accès une personne devrait-elle avoir à son dossier médical si, selon son médecin, il serait nuisible à son état qu'elle sache qu'elle est atteinte d'une maladie mortelle.

Mme Elliott: D'après la *Credit Reporting Act*, quoique le médecin puisse fournir ces renseignements à une agence de crédit avec l'approbation de la personne, la personne n'aura peut-être pas accès à cette information lorsqu'elle consultera son dossier.

M. Beatty: Mais ce que je dis, c'est que à ce moment-ci je ne suis même pas sûr que nous soyons en mesure de rédiger une Loi sur la protection de l'information contenue dans les dossiers médicaux, en comprenant complètement ses implications. Et ce n'est là qu'une infime partie de l'information existante sur une personne. Cela devient insaisissable si l'on élargit le sujet. À ce moment-ci, je ne pense pas que nous ayons l'expérience qui nous permette d'aller aussi loin. À mon sens, il faudra un certain temps avant que nous soyons en mesure de le faire, et nous devrions peut-être y aller petit à petit lorsque le besoin sera évident. Nous pouvons poursuivre pour ce qui est des crimes par ordinateur et dire que si quelqu'un a accès au dossier personnel d'une façon non autorisée, à cause du lacune dans le Code criminel, alors cela constitue de façon évidente une réelle menace à votre vie privée et il faut combler cette lacune maintenant. À ma connaissance on n'a présenté aucun argument contraire qui ait du poids.

Il y a peut-être beaucoup d'autres domaines comme celui-là où nous pouvons agir de façon *ad hoc*. Ma seule hésitation c'est de savoir si à ce moment-ci nous pouvons avoir un projet de Loi sur la vie privée pour le secteur privé et s'il est pratique pour nous de procéder de la sorte.

Mme Elliott: Je présume que dans le cas de vol par ordinateur et dans le domaine de l'établissement de normes et de systèmes de surveillance, vous obtiendriez beaucoup d'informations sur la protection de la vie privée, simplement par cette méthode, en établissant essentiellement l'importance et la pertinence des systèmes et des renseignements personnels.

M. Beatty: Oui. Je pense que votre recommandation d'effectuer une étude est très utile, car elle peut aider à fournir ce cadre d'information à partir duquel on peut travailler.

Bien, je vous remercie beaucoup pour votre très utile mémoire et pour les précisions que vous avez apportées. J'ai beaucoup apprécié cela.

[Text]

The Chairman: Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Yes. I have a couple more questions.

You have indicated that you subscribe, I guess, to the five questions that Privacy Commissioner Inger Hansen would ask with regard to information, on Page 14 of your report. I am wondering, do you consider these all-inclusive or are there other questions that should be asked.

Ms Elliott: We were comfortable with these lists of questions and would be most interested to find any other elaboration that is required at the moment. We agree with Inger Hansen's...

Mr. Robinson (Etobicoke—Lakeshore): Is it your view that any information that would be put on record should be at the consent of the individual?

Ms Elliott: Yes.

Mr. Robinson (Etobicoke—Lakeshore): Or at least with the knowledge of the individual?

Ms Elliott: Yes.

Mr. Robinson (Etobicoke—Lakeshore): Yes to both.

What limits do you think should be set on the dissemination of the information? In other words, if it is given to the police because they are investigating an accident, we will say, or the information is given to a hospital because you are going to have an operation, or something like that, what limits do you think should be set on the information given? Or have you considered this?

Ms Elliott: Except in some cases... Let us back up a bit here... We believe that when you provide information you should know for what it is being used and you should know or be confident that it will be kept secure and confidential and so forth. We recognize that sometimes when you do not provide personal information you do not obtain the service. That happens sometimes with social insurance numbers. That is a good example right there. A recommendation which is not in this brief, per se, but which we are reviewing, is that application forms or any forms that require personal information should be reviewed or, on a voluntary basis, reviewed by human rights commissions and so forth, to ensure that information asked is necessary. It should be made clear what you are providing and what is going to happen to it.

Mr. Robinson (Etobicoke—Lakeshore): All right. Now, the last question I have is the following, and it refers back to the statement that you made when you said, if I have it correctly: "We need some form of protection for the individual from the computer". And when you made that statement, I suppose you got a short answer which was probably, Well, just amend the Criminal Code and provide special legislation. But what do you really see as being the nub of the problem? How do we resolve it? How do you deal with this whole matter, to protect

[Translation]

Le président: Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Oui. J'ai quelques questions de plus.

Vous avez dit entériner les cinq questions que le commissaire à la protection de la vie privée, Inger Hansen, demanderait au sujet de l'information, c'est à la page 14 de Votre rapport. Je me demande si vous considérez que ces questions comprennent tous les aspects ou s'il y en a d'autres qu'on devrait poser.

Mme Elliott: Nous sommes satisfaits de cette liste de questions et nous serions extrêmement intéressés à trouver toutes autres précisions qui seraient nécessaires pour le moment. Nous sommes d'accord avec Inger Hansen...

M. Robinson (Etobicoke—Lakeshore): Estimez-vous que toute information mise dans un dossier devrait l'être avec le consentement de la personne?

Mme Elliott: Oui.

M. Robinson (Etobicoke—Lakeshore): Ou du moins qu'elle en soit informée.

Mme Elliott: Oui.

M. Robinson (Etobicoke—Lakeshore): Oui, aux deux questions.

Selon vous, quelles limites devrait-on imposer à la dissémination de l'information? Autrement dit si l'information est transmise à la police parce qu'elle enquête sur un accident, disons, ou si l'information est transmise à un hôpital parce que vous devez subir une opération ou quelque chose de ce genre, quelle limite, selon vous, devrait-on fixer pour ce qui est de transmettre l'information? Est-ce que vous étudiez la chose?

Mme Elliott: Sauf dans certains cas... Revenons un peu en arrière... nous croyons que lorsque vous fournissez de l'information vous devriez savoir dans quel but et vous devriez savoir ou être convaincu que ces renseignements seront en sécurité, qu'ils seront confidentiels et ainsi de suite. Nous reconnaissons que parfois lorsque vous ne fournissez pas de renseignements personnels, vous n'obtenez pas le service demandé. Cela se produit parfois avec les numéros d'assurance sociale, voilà un bon exemple. Il y a une recommandation qui n'est pas dans le mémoire comme telle, mais que nous étudions présentement, c'est que les formulaires de demandes ou tout formulaire demandant des informations personnelles soient examinés, sur une base volontaire, par les Commissions des droits de la personne et ainsi de suite, pour déterminer si les renseignements demandés sont nécessaires. On devrait préciser également les renseignements que vous fournissez et l'utilisation qu'on en fera.

M. Robinson (Etobicoke—Lakeshore): Très bien. Voici ma dernière question, et je me reporte à une déclaration que vous avez faite lorsque vous avez dit, si j'ai bien compris: «Nous devons, de quelque façon que ce soit, protéger la personne contre l'ordinateur». Lorsque vous avez fait cette déclaration, je présume qu'on vous a répondu, eh bien, modifiez simplement le Code criminel et adoptez une loi spéciale. Mais selon vous quel est réellement le noeud du problème? Comment pouvons-nous le résoudre? Comment peut-on justement

[Texte]

the individual from the computer? Maybe your colleague wants to answer this.

• 1640

Ms Elliott: Maybe she does.

Ms Christine Bisanz (Acting Director of Association Policy and Activities, Consumers' Association of Canada): First of all, I think one critical point we have to make is that the computer is a tool. The computer does not commit theft or fraud, it is the user who is utilizing it and accesses the information—for whatever reason, whether it is authorized or unauthorized—who has the ability to manipulate the computer in whatever way or simply to utilize the information that comes out of it. What we are representing here today is the consumer interest, and the consumer interest in terms of what is put into the computer.

As we have said several times, the computer is being used more and more for more and more purposes, the primary purpose, of course, being the storage of information. I guess the principle here is that the information itself has to be defined and recognized as a thing, or some thing, and when we talk about invasion of privacy, and so on and so forth, it is accessing that thing, that thing about me. If, for example, I submit my social insurance number to a store, or whatever, as an identifying number that they can use, I do not object to their requesting it because I have something to hide, I object to their using it because that information that I provided to obtain a social insurance number in the first place, that thing I have provided, is some thing that has been provided for a particular reason, and not because of any cheque-cashing policies or anything else.

Mr. Robinson (Etobicoke—Lakeshore): In other words, it is not a question of protecting the individual from an inanimate object like a computer, it is protecting the individual from another individual who is using that computer to get information about you that offends your right to privacy.

Ms Elliott: I think I am guilty of a colourful phrase there. I think you have summarized it correctly.

Mr. Robinson (Etobicoke—Lakeshore): Thank you.

The Chairman: Thank you for appearing before us this afternoon and for the fruitful and useful and probably original point of view.

I would like just maybe to have a small comment from my colleague, Mr. Beatty. There are some special provisions in the legislation of Quebec with regard to medical records—their use, how they could be used, to whom they could be given and some sanctions also for the misuse of personal data in medical records. That is in Bill 48. Of course, it may not be generally implemented at each provincial level, but I was wondering how, at the federal level, we could make some intervention in these files, because I do not think it is much of our—of some documents that are of concern to us...—except, of course,

[Traduction]

protéger la personne contre l'ordinateur? Peut-être que votre collègue voudra répondre à cette question.

Mme Elliott: Peut-être qu'elle veut commenter.

Mme Christine Bisanz (directrice suppléante, politique et activités, Association des consommateurs du Canada): D'abord, l'un des points critiques que nous devons établir, c'est que l'ordinateur est un outil. L'ordinateur ne commet pas de vol ni de fraude, c'est l'utilisateur qui s'en sert pour avoir accès à l'information, ou pour quelque autre motif que ce soit, de façon autorisée ou non, qui a la possibilité de manipuler l'ordinateur ou simplement d'utiliser l'information qu'il en retire. Ce que nous représentons aujourd'hui, c'est l'intérêt du consommateur par rapport à ce qui est mis dans l'ordinateur.

Comme nous l'avons déjà dit à de nombreuses reprises, l'ordinateur est de plus en plus utilisé pour de plus en plus de choses, la principale utilisation étant, bien sûr, le stockage d'informations. Je présume que le principe ici, c'est que l'information comme telle doit être définie et reconnue comme une chose ou comme quelque chose, et lorsque nous parlons d'invasion de la vie privée, et ainsi de suite, c'est que l'on permet l'accès à cette chose, cette chose qui contient des renseignements sur moi. Par exemple, si je donne mon numéro d'assurance sociale à un magasin ou ailleurs, comme pièce d'identité qu'ils peuvent utiliser, je ne m'oppose pas à ce qu'ils le demandent parce que j'ai quelque chose à cacher, je m'oppose à ce qu'ils l'utilisent à cause des renseignements que j'ai fournis pour obtenir ce numéro d'assurance sociale au départ, ces renseignements que j'ai fournis l'ont été pour une raison particulière et non à cause de politiques d'encaissement de chèques ou quoi que ce soit d'autre.

M. Robinson (Etobicoke—Lakeshore): Autrement dit, il ne s'agit pas de protéger la personne d'un objet inanimé comme l'ordinateur, mais de protéger la personne contre une autre personne qui utilise cet ordinateur pour obtenir de l'information à votre sujet, information, qui viole vos droits à la vie privée.

Mme Elliott: Je reconnais avoir fait une phrase un peu colorée, je pense que vous avez bien résumé.

M. Robinson (Etobicoke—Lakeshore): Merci.

Le président: Merci d'avoir comparu devant nous cet après-midi et d'avoir donné des points de vues utiles, féconds et probablement originaux, que vous nous avez présentés.

Je voudrais peut-être avoir un petit commentaire de mon collègue, M. Beatty. Il y a des dispositions spéciales dans les lois du Québec concernant les dossiers médicaux... leur utilisation, la façon dont on peut les utiliser, à qui ils devraient être transmis et les sanctions pour une mauvaise utilisation des données personnelles contenues dans les dossiers médicaux. Il s'agit du projet de loi 48, bien sûr, ces dispositions ne s'appliqueront peut-être pas généralement à chaque province, mais je me demandais, au niveau fédéral, si nous pourrions intervenir dans ce domaine, car je ne pense que ce soit vraiment de notre... de certains documents qui nous intéressent... sauf,

[Text]

through the Criminal Code, but there is a limit to the extension of the application of the Criminal Code.

Mr. Beatty: There is also in Ontario a very excellent study that was done on the confidentiality of medical records, which I do not think has led to legislation yet—has it?

Ms Elliott: I do not think so.

The Chairman: Thank you for appearing before us.

Tomorrow we will have Mrs. Susan Nycum, attorney-at-law, from California. I think she is an expert from the United States and I hope that you will be able to attend.

Thank you for coming.

Ms Elliott: Thank you.

Ms Bisanz: Thank you.

[Translation]

bien sûr, par le truchement du Code criminel, mais il y a une limite à l'élargissement du champ d'application du Code criminel.

M. Beatty: Il y a eu aussi une excellente étude effectuée en Ontario sur la confidentialité des dossiers médicaux, mais je ne pense pas que cela ait débouché sur un projet de loi jusqu'ici . . . Est-ce que c'est le cas?

Mme Elliott: Je ne pense pas.

Le président: Merci d'avoir comparu devant nous aujourd'hui.

Demain, nous recevrons M^{me} Susan Nycum, avocate de la Californie. Je pense qu'elle est un expert des États-Unis et j'espère que vous pourrez être là.

Merci d'être venues.

Mme Elliott: Merci.

Mme Bisanz: Merci.



*If undelivered, return COVER ONLY to
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9*

*En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9*

WITNESSES—TÉMOINS

From the Consumers' Association of Canada:

Ms. Christine Bisanz, Acting Director of Association and
Activities;

Ms. Christine Elliott, Member, Ontario Branch.

De l'Association canadienne des consommateurs:

M^{lle} Christine Bisanz, Directrice suppléante, Politique et
Activités;

M^{lle} Christine Elliott, Membre, section Ontario.

HOUSE OF COMMONS

Issue No. 15

Wednesday, June 1st, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 15

Le mercredi 1^{er} juin 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

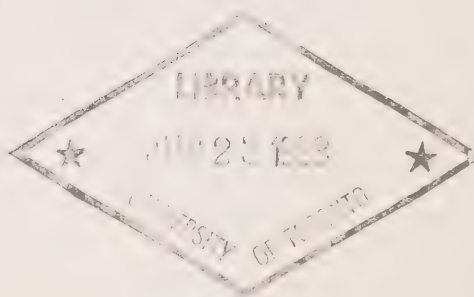
Questions relatives à l'ordre de renvoi

WITNESS:

(See back cover)

TÉMOIN:

(Voir à l'endos)



First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trrente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, JUNE 1, 1983
(17)

[Text]

The Sub-committee on computer crime met this day at 3:46 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witness: Mrs. Susan H. Nycum, Attorney-at-Law, from Gaston, Snow and Ely Bartlett, Palo Alto, California.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1.*)

On motion of Mr. Beatty, it was agreed,—That a per diem allowance in accordance with the scale approved by the Speaker, be paid to Mrs. Susan H. Nycum, Attorney-at-Law, from Palo Alto, California, in relation with her appearance before the Sub-Committee on computer crime.

The witness made a statement and answered questions.

On motion of Mr. Robinson (*Etobicoke—Lakeshore*), it was ordered,—That the testimony by Donn B. Parker and Susan H. Nycum on computer crime before the U.S. House of Representatives Sub-Committee of the Judiciary Committee on Constitutional and Civil Rights, September 23, 1982, Washington, D.C., be printed as an appendix to this day's Minutes of Proceedings and Evidence (*See Appendix "COMP-3"*.)

At 5:29 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 1^{er} JUIN 1983
(17)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h46, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoin: M^{me} Susan H. Nycum, avocate, de «Gaston, Snow and Ely Bartlett», Palo Alto, Californie.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal, mardi le 15 mars 1983, fascicule n° 1.*)

Sur motion de M. Beatty, il est convenu,—Qu'une indemnité quotidienne selon une échelle approuvée par l'Orateur, soit versée à M^{me} Susan H. Nycum, avocate de Palo Alto, Californie, relativement à sa comparution devant le Sous-comité sur les infractions relatives aux ordinateurs.

Le témoin fait une déclaration et répond aux questions.

Sur motion de M. Robinson (*Etobicoke—Lakeshore*), il est ordonné,—Que le témoignage de Donn B. Parker et de Susan H. Nycum sur la criminalité informatique fait devant le «Sub-committee on the Judiciary Committee on Constitutional and Civil Rights» de la Chambre des représentants des États-Unis, le 23 septembre 1982, à Washington (D.C.), soit imprimé en appendice aux procès-verbaux et témoignages de ce jour. (*Voir appendice "COMP-3"*.)

A 17h29, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Wednesday, June 1, 1983

• 1546

Le président: Le Sous-comité reprend l'étude de son ordre de renvoi concernant les infractions relatives aux ordinateurs.

Aujourd'hui, nous recevons M^{me} Susan Nycum, avocate de Palo Alto en Californie, qui a accepté de bien vouloir partager avec nous son expérience dans le domaine.

Avant de souhaiter la bienvenue à M^{me} Nycum, je voudrais faire une suggestion à mes collègues du Comité,

and ask if they would support a motion that a per diem allowance, in accordance with the scale approved by the Speaker, be paid to Mrs. Susan Nycum, attorney-at-law from Palo Alto, California, in relation with her appearance before the Subcommittee on Computer Crime. Since Mrs. Nycum is coming from California and has to take three days to appear before us, I think it would be at least a little decent for the House of Commons to ask for at least a small fee, which the Speaker has the discretion to pay. The actual scale is \$50 per day.

So do I have someone to move the motion?

Mr. Beatty: I would be pleased to move the motion.

Mr. Robinson (Etobicoke—Lakeshore): I second the motion.

The Chairman: It is moved by Mr. Beatty and seconded by Mr. Robinson.

Motion agreed to.

The Chairman: I would like to welcome Mrs. Nycum, who will give us the benefit of all her research and experience in the field of computer crime. We will hear your testimony and then my colleagues and I might ask a few questions, if you do not mind.

Mrs. Susan Nycum (Attorney-at-Law, Palo Alto, California): It would be my pleasure. I thought what I might do is give you some information I had understood you were particularly interested in hearing and then invite questions on any other aspect of the subject on which you would be further interested in knowing my views or experience.

My name is Susan Hubbell Nycum. I am a partner in the United States law firm of Gaston, Snow and Ely Partlett. I am resident in the Palo Alto, California, office of that firm. I am the partner in charge of the high technology group of the firm nationwide, but I should say the opinions expressed today are my own and do not necessarily reflect those of either of our partners or any of the clients of the firm.

I am currently Vice-President of the Computer Law Association. I am a member of the American Bar Association committee to the National Conference of Lawyers and

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mercredi 1^{er} juin, 1983

The Chairman: The sub-committee resumes consideration of its order of reference respecting computer crime.

Our witness today is Mrs. Susan Nycum, Attorney-at-Law from Palo Alto, California, who agreed to share with us her experience in this field.

Before welcoming Mrs. Nycum, I would like to make a suggestion to my colleagues from the committee.

et leur demander s'ils seraient prêts à appuyer une motion prévoyant l'octroi d'un per diem conformément à l'échelle approuvée par la présidente de la Chambre, en faveur de M^{me} Susan Nycum, avocate de Palo Alto, en Californie, qui comparaît devant le Sous-comité des infractions relatives aux ordinateurs. Étant donné que M^{me} Nycum vient de Californie et a pris trois jours de congé pour comparaître, il conviendrait que la Chambre lui verse un petit montant de \$50 par jour.

Y a-t-il quelqu'un qui veut proposer la motion?

M. Beatty: Je serais heureux de le faire.

M. Robinson (Etobicoke—Lakeshore): J'appuie la motion.

Le président: Proposé par M. Beatty et appuyé par M. Robinson.

La motion est adoptée.

Le président: Je souhaite maintenant la bienvenue à M^{me} Nycum qui nous enrichira du fruit de ses recherches et de son expérience dans le domaine des infractions relatives aux ordinateurs. Nous entendrons votre témoignage, après quoi mes collègues et moi-même vous poseront des questions si cela ne vous dérange pas.

Mme Susan Nycum (avocate, Palo Alto, Californie): J'en serais très heureuse. J'ai pensé que la meilleure façon de procéder serait sans doute de vous donner les renseignements qui pourraient, si je ne me trompe, vous intéresser tout particulièrement, ensuite répondre aux questions que vous pourriez me poser sur tout autre aspect du sujet.

Mon nom est Susan Hubbell Nycum. Je suis associée dans l'étude Gaston, Snow et Ely Partlett. J'habite à Palo Alto en Californie où se trouve cette étude. Je suis responsable du groupe de la haute technologie pour notre firme et ceci à l'échelle de tout le pays, cependant, j'aimerais spécifier que les opinions que j'exprimerai aujourd'hui sont les miennes et ne reflètent pas nécessairement celles de nos associés ou des clients de la firme.

Je suis actuellement vice-présidente de la *Computer Law Association*. Je suis membre du Comité de l'Association du barreau des États-Unis à la *National Conference of Lawyers and Scientists*, (Conférence nationale des avocats et hommes

[Texte]

Scientists, and I am a former chairman of the American Bar Association Section on Science and Technology.

At the international level, recently I have served as a United States State Department delegate to an OECD meeting on national vulnerabilities and shall be attending next week a WIPO meeting in Geneva, which will regard a draft treaty for protection of intellectual property in software.

For the past 14 years, I have been studying computer abuse under a series of grants from the National Science Foundation and the U.S. Department of Justice with my friend and colleague, Donn Parker, as co-principal investigators, and I have recently been serving as a consultant to the Canadian Department of Justice.

The practice in the series of researches that Donn Parker and I have been doing has been to collect and categorize reported incidents of computer abuse, and we have identified computer abuse as those incidents in which a victim could have or did suffer a loss or a perpetrator could have or did achieve a gain. This avoids the notion of using the words "computer crime", when in a technical sense, there may not actually have been a crime.

• 1550

We have a data base of reported incidents of in excess of 1,000 and each year we have investigated in some depth a number of the more representative and sometimes the more, we think, useful of those incidents. When we have performed the in-depth investigation, we have interviewed the persons involved in the activity, including the perpetrator, the victim, the insurers, the law-enforcement personnel and prosecutors, as well as others who may have been involved, such as a trustee in bankruptcy with respect to the equity funding insurance fraud, as an example.

In our experience, the acts that we have looked at in depth—and it tracks with the cases of reported abuses that we have not looked at thoroughly ourselves... fall into four general categories of goal. The first is where the goal is financial fraud or theft. In some cases, there have been massive, multiple, million-dollar frauds and thefts, some resulting in bankruptcies of the targeted company, such as the recent case of Saxon Industries Incorporated, in which there was a large overstatement of inventories by senior management in the multiple millions and the company could not survive the fraud. Sometimes there have been multiple small incidents, such as with the Citibank frauds on the automated teller machines, where individuals were deprived, from their bank accounts, of dollars in the amount of one or two or several hundred at a time. The total loss, including the interest, may be in the low one-hundred thousand dollars.

[Traduction]

de science) et je suis ancienne présidente de la section de la science et de la technologie de l'Association du barreau des États-Unis.

Sur le plan international, j'ai été la déléguée du secrétariat d'État des États-Unis à la réunion de l'OCDE portant sur la vulnérabilité des différentes nations aux infractions relatives aux ordinateurs et je participerai la semaine prochaine à la réunion de l'Organisation mondiale de la propriété intellectuelle à Genève, réunion au cours de laquelle on étudiera un projet de traité en matière de protection de la propriété intellectuelle sur logiciel.

Au cours des 14 dernières années, j'ai étudié les abus commis au moyen d'ordinateurs grâce à une série de subventions de la *National Science Foundation* et du ministère américain de la Justice, avec mon ami et confrère Donn Parker. Nous étions les deux principaux chercheurs et j'ai récemment exercé les fonctions de consultant pour le ministère canadien de la Justice.

De façon générale, mon ami Donn Parker et moi-même avons procédé de la façon suivante: nous avons rassemblé et classé les différents incidents dont on nous avait fait rapport concernant les abus perpétrés à l'aide d'ordinateurs. Nous avons pu identifier de tels abus comme étant des incidents au cours desquels une victime aurait pu ou a été lésée et la personne responsable de cet abus aurait pu en retirer des avantages ou en a retiré. De cette façon, nous évitons d'utiliser l'expression infraction quand, dans un sens strictement technique, il n'y en a peut-être pas eu.

Nous avons une base de données portant sur plus de 1,000 incidents qui nous ont été rapportés et chaque année, nous avons étudié assez en profondeur certains de ces incidents les plus marquants et, à notre avis, les plus utiles. Au cours de nos enquêtes en profondeur, nous avons interviewé les personnes impliquées, l'auteur, la victime, les assureurs, les personnes responsables de l'application de la loi, les procureurs ainsi que toutes les autres personnes en cause comme les syndicats de faillite dans les cas de fraudes en matière d'assurance de capitaux, par exemple.

Selon notre expérience des cas que nous avons étudiés en profondeur, ceux-ci se rangent dans quatre grandes catégories, ce qui est d'ailleurs confirmé par les autres cas que nous n'avons pas étudiés complètement nous-mêmes. De façon générale donc, ces actes visent l'un ou l'autre des quatre buts suivants: tout d'abord, le but recherché peut être la fraude financière ou le vol. Dans certains cas, il y a eu des fraudes massives multiples et représentant des millions de dollars ainsi que des vols qui ont abouti à la faillite de la compagnie faisant l'objet de tels actes. Nous connaissons le cas récent de *Saxon Industries Incorporated* où les cadres supérieurs ont surévalué de plusieurs millions de dollars les stocks de la compagnie qui n'a pas survécu à une telle fraude. Parfois, il y a eu de nombreux incidents d'ordre mineur, comme dans le cas des fraudes commises à *City Bank* sur des caisses automatiques où l'on a volé un, deux ou plusieurs centaines de dollars à la fois sur les comptes bancaires de certaines personnes. La perte

[Text]

Then there has been the second category, where the goal is information fraud or theft. Examples are theft of seismic data, theft of computer programs—some of which, as we know now, are in the neighbourhood of a value of \$1 million or more, depending on what the function of the program is—and sometimes the information has been data on people. As an example, occasionally we find in our data base a repetitive type of crime or abuse, in which a person who has a data bank under his or her control—in, say, a police station function—of people who have been victims of home burglaries uses that information to operate a company that provides insurance to folks who have been victims of home burglaries.

A third category is where the goal is theft of services. Services here generally included computer time, which can either be the raw use of the time or the full selection of associated goods and services that go along with running a commercial service bureau. There have been several cases where people employed in a dedicated service field function within an organization have, on the side, sold that service to outsiders for their personal profit.

The fourth category is where the goal is sabotage of facilities. In the U.S., there was a rash of that during the Viet Nam-Cambodian wars and, most recently, in other countries, the Red Brigade in Italy. The actual goal is to be destructive. In the U.S., more recently, there have been some commercial sabotages taking place between competitors, where a person working for a company has actually set fire to or bombed the facilities of a competitor.

We have also looked at the involvement of the computer and we have found that the computer has been involved in another set of four gross categories.

• 1555

The first is where the target is the computer itself, where either the hardware or the system is actually the result of the fulfilment of the goal. I just mentioned the sabotage; that would be a clear case of where the hardware is the target. Certainly, theft of computers is much easier as they become smaller and components very much simpler, as we move into the micro and now into the pocket-sized computer, just the taking of the tangible property itself.

Less easy to address, particularly from a legal standpoint, is where the target is the computer system. Several years ago, there was an incident in New York City which involved the Metropolitan Life Insurance Company, in which data was being transferred over telephone lines from remote sites into a central computer. Systematically, the remote devices were found not to have transmitted when they had been checked the following day; and it was found that customer engineers, the maintenance people for the computer company which was providing the service to the Metropolitan Life Insurance Company, were disgruntled with the company they worked for

[Translation]

totale, si l'on inclut l'intérêt, représente un peu plus de \$100,000.

Dans la deuxième catégorie, le but recherché est la fraude en matière d'information, le vol de renseignements. Ainsi, l'on vole des données sismiques, des programmes d'ordinateur dont certains valent, comme nous le savons à l'heure actuelle, un million de dollars ou plus selon la fonction du programme, ... et parfois des données concernant certaines personnes. Parfois, nous trouvons dans notre base de données des cas d'infraction ou d'abus commis de manière répétitive où une personne ayant accès à une banque de données, par exemple parce qu'elle travaille pour la police, possède des renseignements sur les victimes de cambriolages, dont elle se sert pour exploiter une compagnie d'assurance-cambriolage, précisément.

Quant à la troisième catégorie, le but recherché est le vol des services. Généralement, il s'agit de voler du temps d'ordinateur ou toute une gamme de biens et services fournis par un bureau de services commerciaux. Nous connaissons plusieurs cas où des personnes travaillant pour une organisation vendent en fraude les services en question.

Dans la quatrième catégorie, le but est le sabotage d'installations. Il y a eu une irruption de ce genre de sabotage aux États-Unis au cours de la guerre du Vietnam et du Cambodge et plus récemment dans d'autres pays, l'Italie notamment, avec l'histoire des Brigades Rouges. Le but en est la destruction. Aux États-Unis, plus récemment, il y a eu quelques sabotages commerciaux entre concurrents; ce qui se passe, c'est qu'un employé d'une compagnie incendie les installations d'un concurrent ou y met une bombe.

Nous avons également étudié la question du point de vue de l'ordinateur lui-même et nous nous sommes rendu compte que l'on pouvait subdiviser cette question en quatre catégories générales.

Tout d'abord, dans la première catégorie, la cible est l'ordinateur lui-même ou tout le système. J'ai parlé du sabotage; il s'agit là d'un cas évident où le matériel devient la cible. Il est évident qu'il devient de plus en plus facile de voler les ordinateurs puisque ceux-ci deviennent plus petits, que leurs éléments sont beaucoup plus simples qu'auparavant. Il ne faut pas oublier que nous sommes maintenant à l'époque du micro-ordinateur ou de l'ordinateur de poche.

Une situation moins claire, particulièrement du point de vue juridique, est celle où la cible est le système d'ordinateur. Il y a quelques années, à New-York, la *Metropolitan Life Insurance Company* acheminait des données par téléphone de sites éloignés à un ordinateur central. Or, on se rendait compte que systématiquement, des données qui devaient avoir été transmises la veille ne l'étaient pas. On s'est rendu compte que les personnes responsables de l'entretien des ordinateurs pour la compagnie qui offrait le service à la *Metropolitan Life* sabotaient tout le système et les données, mais non le matériel. Ces personnes agissaient simplement par ressentiment envers

[Texte]

and so sabotaged, if you will, the system and the data, although nothing was done to the hardware, by finding out the polling sequence or the telephone connection sequence used to get the data transferred from the remote site into the central storage area and processing area and emulating that, only of course, just to emulate the commencement of the cycle, not to receive it in any fashion. Thus there was a tremendous loss of real out-of-pocket services, time and materials by the company, Metropolitan Life Insurance Company, as they attempted to recover from that loss of data being transferred.

This is a type of thing which is a problem, potentially, for other organizations in the U.S., particularly the supermarket chains, where now, increasingly, there is sensing over time of the check-out stands. That data is collected at one particular grocery store and then sent on, perhaps in a daily sequence, over telephone lines.

So that is the first category, where the target is the computer. The computer is represented as the target.

The second is where the target is really the information stored in the computer; and it involves not only the examples of information, fraud and theft but also the case of manipulation of that information.

A large credit reporting agency, TRW in Los Angeles, has several cases where people with poor credit ratings were in collusion with clerks who were inside that information. What they did was pay the clerks money to change the computer records so that their credit rating was vastly improved. Then they could go out and charge a lot more goods and services.

There was an example in our California Motor Vehicle Bureau where a ring which was stealing cars was significantly enhanced by the procedure of giving false owners' certificates on certain cars which had been stolen. Again, it was a clerk who would change the records to indicate that the registration was in the name of the thief. Then, after the car was stolen, in fact—and the clerk knew it to be stolen—but before the authorities knew, he would then change those records back to show the original owner. In the meantime, the person who was the thief would have gone in and said he had lost the copy of his registration; and the clerk who was responsible for that area would check the computer records and see that he, indeed, was the true owner and would issue a so-called replacement registration for him, which he could then use to sell the car.

• 1600

So there are numbers of different times when the information within the computer has great value and the computer is used in the fraud as a storage device, really.

A third case is where the computer is the perpetrating device. This happens in a number of different forms. The first one is input; the next one is output; and the third is processing. There is a term of art, or a jargon term, which is called "data diddling". We have found that the type of crime we see the most of is at the input end, where the data diddling is done by

[Traduction]

la compagnie qui les employait. Elles avaient trouvé la séquence des communications téléphoniques nécessaire à l'acheminement des données de l'endroit éloigné à la réserve centrale et aux installations de traitement et pouvaient reproduire le début du cycle, même si elles ne pouvaient recevoir des informations d'aucune façon. Il y a donc eu une perte énorme de services, de temps et de données pour la *Metropolitan Life* quand cette compagnie a voulu essayer de récupérer une telle perte.

C'est le genre de problèmes que peuvent rencontrer d'autres entreprises américaines, particulièrement les chaînes de supermarchés où les données obtenues aux différentes caisses d'un magasin sont rassemblées puis acheminées parfois de façon quotidienne par lignes téléphoniques.

Il s'agit donc de la première catégorie où la cible est l'ordinateur.

Dans une deuxième catégorie, la cible est l'information entreposée dans l'ordinateur. Nous avons à cet égard des exemples de fraudes et vols de renseignements mais également de manipulation des renseignements.

La TRW de Los Angeles, entreprise qui rassemble des informations concernant le crédit des particuliers, a connu plusieurs incidents où des personnes ayant une mauvaise cote de crédit s'étaient abouchées avec des commis de TRW, leur avaient offert un pot-de-vie afin de modifier les données de l'ordinateur concernant leur cote de crédit. De cette façon, leur cote était nettement améliorée et ces personnes pouvaient continuer à acheter à crédit de nombreux biens et service.

Le Bureau d'immatriculation des automobiles de Californie a été le théâtre d'activités illégales; en effet, un réseau responsable de vols de voitures recevait l'aide d'un commis qui modifiait les dossiers d'immatriculation des véhicules automobiles. Ce commis inscrivait le véhicule au nom du voleur. Une fois la voiture volée mais avant que les autorités n'aient été mises au courant, ce commis modifiait à nouveau les dossiers pour y faire figurer le nom du vrai propriétaire. Entre temps, le voleur se présentait au bureau pour demander un duplicata de sa carte d'immatriculation, ce qui lui permettait de vendre la voiture.

Dans de nombreux cas, les renseignements contenus dans l'ordinateur sont de grande valeur et l'on se sert de celui-ci comme d'une mémoire.

Quant à la troisième catégorie, l'ordinateur sert à commettre la fraude. Cela se passe de différentes façons, au moment de l'entrée, de la sortie, ou du traitement. Il s'agit tout simplement de jouer avec les données. Le plus souvent, on joue avec les documents de base comme dans le cas que je viens de vous décrire il y a quelques instants. Ainsi, au moment de

[Text]

people like the ones I just described a few minutes ago, where particularly a clerk, prior to the processing, changes the input which will be the basis of the computer processing.

The largest one that we know of to date was the Equity Funding Insurance fraud of \$2 billion several years ago in Los Angeles. Here the computer was used to mask the fact that there were no insurance policies; but if the auditor looked for one, then the computerized records were carefully fabricated at what were called all-night fraud parties . . . to keep, I guess, the people working hard—and then the paper records and the computer records would actually match.

More recently, a year or so ago, J. Walter Thompson Co., one of our very large advertising agencies, suffered an extreme loss on its books when it was discovered that one of its divisions which had been reported to be extremely profitable had in fact been routinely overstating its profitability. That was done by the manager of that section or division simply putting false information into the computer. It is curious that when that was discovered, the external auditors for that company paid voluntarily . . . that is, not pursuant to any court order—\$1.2 million to the company for, we assume, their failure to have detected what was going on.

One of the other interesting aspects of that situation was that the person was terminated and immediately brought suit for disparagement against the company in the amount of \$1.2 million. So the victim company potentially will suffer twice: once on its earnings statements, and secondly because of the way the case was allegedly handled when the fraud was discovered.

In the output category of abuses, where the computer is the perpetrating device, there is the very, very simple example of the programmer who was in the machine room, the operations part of the function, when his salary cheque was being printed, and he simply leaned back against the machine that was doing the printing and hit the repeat button so multiple copies of his cheque were printed at the same time. I comment on that one first as a clear example of how this can be done. But he did a very foolish thing thereafter, which is why we know about it: he took all those copies to the very same teller in a bank to cash at the same time, and attracted attention to himself.

Both of these categories—the input and the output—do not require an enormous amount of technical ability to perpetrate. In the last case, where the processing is the scene of the crime, or the way in which the computer is involved, there is a need to have technical competence. Those include the salami technique, or the small slices of money siphoned off a lot of bank accounts over time. They include the Trojan horses, wherein dangerous computer programs are lodged inside innocuous ones and at the appropriate time, very like the soldiers inside the horse, they come out and take over the computer. A number of these have been discovered.

[Translation]

l'entrée, un commis modifie les données qui serviront de base au traitement.

Le cas le plus notoire jusqu'à présent est celui de l'*Equity Funding Insurance* où il y a quelques années à Los Angeles, on a commis une fraude s'élevant à 2 milliards de dollars. L'ordinateur a servi à masquer le fait qu'il n'existait aucune police d'assurance. Cependant, des dossiers informatisés avaient été fabriqués avec soin au cours de sessions nocturnes et ceci, à l'intention du vérificateur.

Plus récemment, il y a un an environ, l'une de nos agences de publicité les plus importantes, la J. Walter Thompson Co., a dû essuyer une perte comptable très importante lorsqu'on a découvert qu'une de ses divisions dont on croyait qu'elle réalisait des bénéfices très importants avait en fait surestimé ses bénéfices. En fait, son directeur introduisait de faux renseignements dans l'ordinateur. La chose curieuse, c'est que lorsque ce pot aux roses a été découvert, les vérificateurs externes de la compagnie ont versé de façon volontaire 1.2 million de dollars à celle-ci, c'est-à-dire sans y avoir été forcés par une injonction de la cour; nous supposons qu'ils faisaient de cette façon amende honorable pour n'avoir pas remarqué la fraude.

Un autre aspect intéressant de ce cas est que l'auteur de cette fraude, après avoir été démis de ses fonctions, a immédiatement intenté des poursuites contre la compagnie pour un montant de 1.2 million de dollars. Ainsi donc la compagnie victime de cette fraude pourrait souffrir deux fois, une première fois pour falsification de ses états de bénéfices, deuxièmement, à cause de la façon dont l'affaire a été traitée lorsque la fraude a été découverte.

Dans le cas où l'abus est commis grâce à l'ordinateur, on peut citer l'exemple extrêmement simple du programmeur qui se trouvait près de celui-ci lorsque son chèque de paie était imprimé. Il s'est appuyé contre la machine et a déclenché le bouton servant à imprimer de multiples exemplaires de son chèque. Vous voyez donc bien clairement comment une telle fraude peut être perpétrée. Cependant, cet employé n'a pas été très intelligent, et c'est la raison pour laquelle nous sommes au courant de ce cas, car il a voulu encaisser tous ses chèques au même guichet d'une même banque en même temps, ce qui a attiré l'attention.

Les fraudes rentrant dans ces deux catégories, que l'on pourrait qualifier de fraudes à l'entrée ou à la sortie, ne nécessitent pas de vastes connaissances techniques, ce qui n'est cependant pas le cas pour les infractions commises pendant le traitement. On peut parler dans ce contexte de la technique salami, des petits montants d'argent détournés au cours d'une longue période de temps de différents comptes en banque. Il y a également la technique du cheval de Troie où des programmes d'ordinateur dangereux sont incorporés à des programmes tout à fait inoffensifs et d'où sortent les soldats à un moment donné pour assumer le contrôle de l'ordinateur. Un nombre de cas de ce genre ont été découverts.

[Texte]

[Traduction]

• 1605

As we get more and more technically elaborate and elegant in our processing capabilities, we sometimes get more and more elaborate nooks and crannies in which problems can occur. If a person who is looking for such a thing is clever enough, be he a student or someone with a particular financial desire, he can take advantage of these little nooks and crannies. Two examples come to mind. The first is one in which a university student actually found a way to place a dangerous computer program inside an innocuous one by writing it inside a utility or program which was designed to save some time for people who would use it. He placed it in the university's user library which anyone could access. Certain people who used it had high authority within the computer system; they could get anywhere in the computer system. So by the nature of who they were, they could bypass all the locks and controls designed for keeping ordinary users out. These would be people who worked inside the systems group in the centre.

When one of them with the requisite level of authority used that innocuous utility program, the program that was inside the dangerous one sensed that and, almost like the knock on the side of the Trojan horse, that dangerous computer program got out into the main system and really took over the main system which was being used. Also, when it did take over the system, it planted in the system a time bomb, so to speak, a logic bomb which at a time in the future was designed to crash the system. Then in its last act, it destroyed all the evidence that had been there at all.

The only way this was found was when a maintenance programmer had to look at a section of the computer code which ran the system. He knew it so well that he saw something was different about it. And when they looked at what was different, they discovered this program. The program was, in fact, designed for a time when the student would not be present, to take over the computer system and to print out some joke or statement to the effect that it had been crashed by someone who had done it intentionally and who was a very clever person.

That type of thing is very much a customary thing, unhappily, in universities in the U.S.A. At least, 10 years ago it was, and we have no evidence that students are less interested in capers of that sort than they were. The epilogue to that story is that the gentleman who was the student is now a member of the faculty of the school on which he was attempting to perpetrate that hoax. And by the way, this is a repeatable situation. Very often the intelligence of the people who perpetrate these types of things, when they are not done for financial gain, is so intriguing to the victim that the victim turns around and hires that person.

The success of those people, once they are hired, has not been uniformly good. It is said that it has changed the person from being an outsider, or someone who is engaged in larceny, more to being an insider and one who is converting the goods that he has been entrusted with.

Plus nos capacités de traitement deviennent complexes, plus il peut se produire des failles qui peuvent par la suite poser des problèmes. En effet, si quelqu'un de suffisamment rusé est aux aguets de telles failles, qu'il soit étudiant ou qu'il désire s'approprier de l'argent, il peut en tirer parti. Deux exemples me viennent à l'esprit. Tout d'abord, le cas d'un étudiant universitaire qui a trouvé un moyen d'incorporer un programme dangereux dans un programme tout à fait inoffensif, dont le but était de faire gagner du temps aux utilisateurs. Il a ensuite placé ce programme à la bibliothèque de l'université à laquelle tout le monde pouvait avoir accès. Certains utilisateurs avaient une haute cote de sécurité dans le système d'ordinateur et pouvaient donc avoir accès au système contrairement à des utilisateurs ordinaires. Il s'agissait de personnes qui travaillaient au sein du groupe informatique au centre.

Lorsqu'une de ces personnes ayant la cote de sécurité s'est servie de ce programme utilitaire tout à fait ordinaire, le programme dangereux qui y avait été incorporé a été déclenché; on pourrait même dire qu'il a déclenché une bombe à retardement dont le but était de faire s'écrouler le système à un moment précis de l'avenir. Après quoi, le programme détruirait toutes les pièces à conviction.

La raison pour laquelle cet incident a été découvert est qu'un programmeur chargé de l'entretien s'est attardé sur le code du système. Comme il le connaissait bien, il a senti quelque chose de louche et est tombé sur le programme en question. Celui-ci avait été conçu pour le moment où l'étudiant ne serait plus à l'université et avait pour but de contrôler le système puis d'imprimer une déclaration amusante révélant que tout le système avait été anéanti de façon intentionnelle par une personne très intelligente.

Ce genre de choses se passent malheureusement très souvent dans les universités américaines. Mon histoire se passait il y a dix ans et rien ne prouve que les étudiants aiment moins à l'heure actuelle se prêter à ce genre de farces. L'épilogue de cette histoire est la suivante: L'étudiant fait maintenant partie de la faculté contre laquelle il avait monté ce canular. Il faut dire en passant que cette situation se répète souvent et que très souvent la victime est fascinée par l'intelligence des auteurs de telles actions d'éclat, sauf quand ils agissent pour des raisons financières, et très souvent la victime finit par engager la personne en question.

Cependant, cela ne se révèle pas toujours une bonne chose puisque l'on peut faire de quelqu'un qui se sent tout à fait extérieur à l'entreprise ou de quelqu'un qui était engagé dans des activités illicites, quelqu'un qui participe à la vie de l'entreprise et à qui l'on fait confiance.

[Text]

The last category where the computer is involved is where the computer is a symbol—something not necessarily actually involved but somehow associated with it. Sometimes it has been used as intimidation. The computer printed it out; therefore, it is correct; therefore, you must agree with the position taken.

• 1610

As I said, these are computer abuses, not necessarily crimes, and we can think of no situation to date in which such an intimidation has actually risen to where we might consider the appropriate sanction to be a criminal sanction.

But there have been some frauds in which the computer has been used or not used which do appear to be actionable. The most recent case is a situation in which a company won a very large contract with the U.S. federal government. It had not been able to deliver on the contract so it used another box from another company and put its name on it and there was nothing inside it. It was a real fraud that there was any computer involved at all. There was a legal research service in New York which advertised that it had used computers in doing legal research and retrieval. No one could ever go to see the system; one was always greeted at the door and never got inside, until finally there was an exposure, which was that the so-called computers were just a number of underpaid law students, quickly, as fast as they could, doing legal research, which then was typed out on what looked like computer printout. Definitely a hoax in that situation.

The last area in which the computer is a symbol is when something goes wrong and the computer, instead of being used to intimidate, is used as a scapegoat: Oh well, it was simply a computer error. There have been situations in the U.S. where usurious amounts of interest have been charged by banks, where people have been denied insurance coverage, where people have had their cars repossessed when they have in fact paid and where heat and other necessities have been turned off because of erroneous understanding that the computer indicates that these people have not paid their bills. Again the defence has been to say: Well, we did not intend it; it was simply a computer error. More and more judges are finding that this is not an error of an independent agency, or some sort of intervening act of God, but something that is a negligent failure on the part of the person who is providing the service.

We have also learned something in the course of our investigations about the types of people who are involved. The types of perpetrators have changed somewhat over the years. In the earlier days, when computers were largely in the universities, research centres and highly controlled areas of major organizations, and where they were typically large mainframes and centrally located, there was a different profile than we are seeing and expect to continue to see in the future. In those days, and still today, we have not seen a large number of career criminals. We have seen instead students, clerks, senior executives, housewives and people who normally are considered first offenders who are not at all the sort that is associated with repeating criminals.

[Translation]

Quant à la dernière catégorie, l'ordinateur est considéré comme un symbole. On ne se sert pas nécessairement de lui, mais il sert d'une façon ou d'une autre, pour intimider, par exemple. Ainsi, on peut faire imprimer à l'ordinateur toutes sortes de choses et intimider de cette façon.

Comme je l'ai dit, il s'agit là d'abus, mais pas nécessairement d'infractions et nous ne pouvons penser à aucune situation jusqu'à présent où l'intimidation a donné lieu à une situation où la peine à infliger aurait pu relever du Code criminel.

Cependant il existe des fraudes qui pourraient donner lieu à poursuite en justice. Le cas le plus récent est celui d'une compagnie qui a décroché un contrat très important du gouvernement fédéral américain, mais n'a pu respecter ses engagements et s'est servi du nom d'une autre compagnie. Il s'agissait d'une véritable fraude au moyen d'un ordinateur. Il y a également le cas d'un service de recherche juridique de New York qui faisait la publicité de services de recherche informatisée. Cependant, personne ne pouvait jamais s'approcher de son fameux système. En fait, il s'agissait d'un service employant des étudiants en droit pour faire la recherche, qui était ensuite tapée sur ce qui semblait être des sorties d'imprimante. Il s'agissait véritablement d'un canular.

Un autre cas où l'ordinateur peut être utilisé comme un symbole est celui où il sert en fait de bouc émissaire. Il s'est produit des situations aux États-Unis où des banques ont imposés des intérêts usuriers, ou certaines personnes se sont vu refuser des contrats d'assurance, où des voitures ont été saisies alors qu'elles avaient été payées, où les services de commodités publiques ont été interrompus parce que l'ordinateur aurait indiqué que ces personnes n'avaient pas payé leurs factures. On s'est alors caché derrière l'ordinateur pour dire que c'était lui qui avait fait une erreur. De plus en plus fréquemment, les juges se rendent compte qu'il ne s'agit pas là d'une erreur mais plutôt d'une négligence, d'un manquement de la part des institutions fournissant les services.

Quant au genre de personnes en cause, nos recherches ont révélé ce qui suit: il s'est produit une évolution au cours des années quant au genre de personnes qui commettent la fraude. Au début de l'ère électronique, quand les ordinateurs se trouvaient surtout dans les universités, les centres de recherche et des endroits très surveillés d'organisations importantes, quand les ordinateurs étaient d'une taille imposante et situés dans un endroit central, les personnes commettant les fraudes étaient très différentes de celles que nous connaissons aujourd'hui. Dans le passé comme aujourd'hui, il n'y a pas un nombre important de criminels ayant pour ainsi dire fait carrière dans ce genre de fraudes. Il s'agit plutôt d'étudiants, de commis, de cadres supérieurs, de femmes de ménage et de

[Texte]

These have been young people because the phenomenon of computing has come recently and most older folk have not been exposed to it early enough to affect their career. So the ages have tended to be from 18 to the early 30s, except for the people involved in financial institutions, where the age has been higher, and indeed in the massive frauds where senior executives have been involved.

The profile shows these people to be very intelligent, to be hard working, to be generally moral people, to have the fascination . . . or a game-playing approach to the computer: it is sometimes regarded as a challenge to out-think it or find its flaws. There have been people who have been severely tempted. Mr. Rifkin, who stole \$10 million from Security Pacific National Bank, said to us that the reason he did it was that every day in his job he passed what looked to him like a little pile of money sitting unguarded in front of him. Finally one day, he just could not resist and actually took what he represented as the pile of money.

• 1615

Some of these people have had unshareable problems that somehow they felt the computer could help them solve, and we have in our annals a number of rather sad situations of people who used the computer as a way to take care of something that was just beyond their capability otherwise. There was a gentleman who stole a million dollars from Union Dime Savings, because he was a compulsive gambler and he had gotten to the point that he needed extra dollars to take care of his gambling debts as one such example.

Now, as the computer enters the marketplace in the form of the personal, or desk-top, or hand-held, or pocket-size computer which can communicate or not as it chooses, whereas its owners choose, we find something that one commentator has referred to as the democratization of computer crime. Instead of being the province of the very skilled, it is now possible for the business person to know enough about computing to perpetrate a fraud, and indeed it is my thought that possibly the incidence, the numbers of incidents, may increase, because the difficulty with the Rifkins and others were that although they can manipulate the system, they did not know enough about the business they were involved in to know how to get the asset out of the computer system, which may be referred to as a closed environment or a closed loop, into their pockets.

Some of the bank criminals did very stupid things. They would very cleverly put all the money received from the "salomy" technique into one or two accounts and then they would have to figure out how to get the money from the account into their pocket. One person having cleverly gotten the task to the point of putting the money into the account got his wife to drive up to the same drive-up teller in the same car several times a day. They thought they were clever by having her change the colour of her hair with various wigs, but they

[Traduction]

personnes qui commettent un crime pour la première fois et que l'on n'associe pas généralement à des récidivistes.

La plupart du temps, il s'agit de jeunes personnes, étant donné que les ordinateurs sont relativement récents. Il s'agit donc de personnes d'un groupe d'âge allant de 18 ans au début de la trentaine sauf dans le cas des personnes impliquées dans la fraude financière et qui sont, elles, plus âgées. Il s'agit notamment de cadres supérieurs.

Généralement ces personnes sont très intelligentes, travailleuses, elles ont un sens moral, elles sont fascinées par l'ordinateur avec lequel elles entrent pour ainsi dire en concurrence. Les tentations peuvent être très grandes. M. Rifkin, qui a volé 10 millions de dollars de la *Security Pacific National Bank*, nous a révélé que la raison pour laquelle il avait commis un tel forfait est que tous les jours il était confronté à des sommes d'argent au sujet desquelles il semblait n'y avoir aucun contrôle. Finalement, un jour, il n'a pas pu résister et il a pris ce qui constituait pour lui un tas d'argent.

Certaines de ces personnes ont des problèmes qu'elles ne veulent partager avec personne et elles pensent que l'ordinateur pourrait les aider à les résoudre. Nous avons dans nos annales un certain nombre de cas plutôt tristes, où des gens se sont servis d'ordinateurs pour essayer de régler un problème qui dépasse leur possibilité. Il y a par exemple un type qui a volé 1 million de dollars de la *Union Dime Savings*. Il était un joueur compulsif et il en est arrivé à un point où il a eu besoin d'argent supplémentaire pour régler ses dettes. Voilà un exemple.

Maintenant, avec l'arrivée sur le marché d'ordinateurs que l'on peut mettre sur son bureau ou même dans sa poche, d'ordinateurs qui peuvent communiquer ou ne pas communiquer, à leur guise ou plutôt à la guise du propriétaire, on constate un phénomène qualifié par un commentateur de démocratisation des crimes relatifs aux ordinateurs. Autrefois, cela n'était à la portée que des gens très doués, mais à l'heure actuelle, un homme ou une femme d'affaires peut être suffisamment au courant de l'informatique pour pouvoir commettre une fraude. Je pense d'ailleurs qu'il est fort possible que l'incidence de ces crimes augmentera, parce que le problème avec les gens comme Rifkin et les autres, c'est que bien qu'ils aient pu manipuler le système, ils n'étaient pas suffisamment au courant des rouages de leur boîte pour trouver le moyen de sortir l'argent du système informatique, qui peut être qualifié de milieu ou de boucle fermée.

Un certain nombre de voleurs dans les banques ont fait des choses tout à fait stupides. Ils versaient très ingénieusement tout l'argent qu'ils avaient récupéré grâce à la technique «salami» dans un ou deux comptes, ils devaient ensuite trouver le moyen de sortir l'argent du compte pour le mettre dans leur poche. Je connais le cas d'une personne qui a réussi à mettre tout l'argent dans un compte, puis il a demandé à sa femme de se pointer plusieurs fois par jour dans la même voiture devant le même guichet. Ils ont été assez astucieux pour prévoir des

[Text]

never thought about the same automobile. There are other similar things where the perpetrator was discovered because of the lack of sophistication in how to really get the money into his own hands.

But now with these personal desk-top computers in the possession of individual account executives and broker dealer organizations, individuals who are writing insurance and increasingly people in the retail establishments, and now with home banking terminals even into the living room of the end user who may leave home and his terminal may be accessed by a person who is breaking in to get the ordinary services and goods that he may have left behind, there is a tremendous broader group of folks who will have the knowledge, skills and access to get the asset to start with and then will know how to capitalize on the money or asset that they have released from the computer system.

As you know, the U.S. has implemented a number of different laws at the state level which I see you have very thoughtfully analysed. It will vary depending on the jurisdiction whether it is an omnibus law to try to address computer abuse as a crime in various U.S. jurisdictions or whether it will be targeted to a particular difficulty which that jurisdiction has faced, which is the case for example in Colorado, or whether there will be an attempt to change the definition of property in a particular state to effect the changes that are perceived as necessary in that jurisdiction.

At the federal level we have had a number of bills introduced, most recently of course H.R. 1092 by Representative Nelson, but to date none has passed. At the federal level we have a number of very effective existing statutes in the form particularly of our wire fraud and our mail fraud statute and in a criminal provision in our copyright law and several criminal provisions in the financial services area, so the fate of 1092 is not clear.

• 1620

However, the states are continuing to actively introduce, and a number are continuing to pass, legislation directed toward this area. I am informed that in Sweden, Norway, the U.K. and Germany there have been laws passed which have bearing on computer crime.

This concludes my prepared remarks. At this point I would be happy to address other questions you may have.

The Chairman: Thank you, Mrs. Nycum. Who would like to begin? Mr. Beatty.

Mr. Beatty: Thank you, Madam Chairman. Let me first of all thank Mrs. Nycum for her very helpful survey. I get the feeling that our minutes may be very much in demand for people looking for ideas on computer crime business.

The first question I would like to ask you relates to the incidence of computer crime, as I understand that you are working with Don Parker. Some of the testimony we previ-

[Translation]

perruques de couleurs différentes, mais ils n'avaient jamais pensé à la voiture. Et il y a d'autres cas semblables où le criminel a été repéré parce que le système qu'il avait prévu pour récupérer l'argent n'était pas assez sophistiqué.

Mais avec les ordinateurs personnels de bureau que se procurent maintenant des comptables et des courtiers, des assureurs et des gens qui travaillent dans des commerces, et avec l'arrivée dans les salons du pays des terminaux de banque... l'utilisateur peut être absent de chez lui et une personne qui pénètre dans sa maison pour voler des services ou biens ordinaires qu'il a laissés derrière lui, peut se servir de son terminal... il y a de plus en plus de gens qui ont les connaissances, les compétences et les possibilités d'accès nécessaires pour pouvoir sortir de l'argent ou des données d'un système informatique et qui savent quoi en faire.

Comme vous le savez, les États-Unis ont adopté un certain nombre de lois au niveau des États, et je constate que vous les avez analysées de très près. Ces lois varieront en fonction de la juridiction; il peut s'agir d'une loi omnibus visant à traiter la truandique comme un crime dans diverses juridictions américaines; il peut également s'agir d'une loi qui vise à régler un problème particulier auquel s'est trouvée confronter la juridiction concernée; je songe notamment au Colorado, ou encore, il se peut que l'on essaie de modifier la définition de ce qu'est la propriété dans un État particulier afin d'apporter à la loi des changements qui sont perçus comme étant nécessaires.

Au niveau fédéral, plusieurs projets de loi ont été déposés, le plus récent étant bien sûr le H.R. 1092, qui a été déposé par M. Nelson, mais qui n'a pas encore été adopté. Au niveau fédéral, il existe un certain nombre de statuts très efficaces qui s'appliquent par exemple à la fraude en matière de télégramme et à la fraude postale, et il y a également une disposition criminelle dans notre Loi sur le droit d'auteur et plusieurs dispositions criminelles dans le domaine des services financiers. Le sort du Bill 1092 demeure donc toujours incertain.

Quoi qu'il en soit, les différents États continuent de proposer et d'adopter un certain nombre de lois dans ce domaine. Et d'après les renseignements dont je dispose, la Suède, la Norvège, le Royaume-Uni et l'Allemagne ont tous adopté des lois portant sur les infractions relatives aux ordinateurs.

J'en ai terminé avec l'exposé que je voulais faire. Je répondrai avec plaisir à toutes vos questions.

Le président: Merci, madame Nycum. Qui aimerait commencer? Monsieur Beatty.

M. Beatty: Merci, madame le président. J'aimerais tout d'abord remercier M^{me} Nycum pour son tour d'horizon très utile. J'ai l'impression que les procès-verbaux de nos réunions seraient très demandés par des gens qui veulent avoir des idées sur des crimes qu'ils pourraient commettre avec des ordinateurs.

D'après ce que j'ai compris, vous travaillez avec Don Parker, et j'aimerais tout d'abord vous poser une question au sujet de l'incidence des crimes relatifs aux ordinateurs. Un certain

[Texte]

ously had before the committee contested some of the figures given as to the extent of computer crime, and particularly contested the iceberg theory of computer crime propounded by Mr. Parker. When we had testimony from Mr. Peter Ward of Peat, Marwick and Partners, in particular he picked up on Mr. Parker's work and said:

One of the favourite quotes in computer crime is that over 85% of computer crime goes unreported. The last time I heard that, it was the Solicitor General of Ontario sitting next to me at an Ontario provincial police computer crime seminar who provided that information. But these are just three comments from what we believe is the mythology that surrounds computer crime. I think that, as in Greek mythology, we should go back to the source to find out where they came from. I will pick the last one and read a paragraph from a letter by Mr. Don Parker. I believe Mr. Parker's name is probably contained in a lot of literature you have read.

In my book *Crime By Computer* I explain that 85% figure

and then he interjects

and I think if you follow back, by the way, that 85% figure you always find that Mr. Parker is the source of origin.

Based on the study of reported violent crime in Detroit, a more recent study in Los Angeles showed the same. I have reasoned that probably fewer white-collar crimes than violent crimes are reported. Therefore, it is likely that more than 85% of computer crimes go unreported.

Mr. Ward then picks up on that and argues that one perhaps cannot analogize from violent crime.

He then goes on to say:

These are verifiable facts, that approximately 75 reported world-wide cases of computer abuse have occurred each year.

I would like to stress the one word "reported" in that. The number of reported cases appears to be levelling off. In fact, if you look at charts in Mr. Parker's books recently, and in some of the material produced by the Stanford Research Institute, the earlier mid-1970s predictions of phenomenal growth in computer crime were not met during the late 1970s. The same information shows that the average annual reported loss is approximately \$40 million, again on a world-wide basis.

Finally, another fact is that Ontario Provincial Police Inspector Campbell of the anti-rackets branch conducted a survey, I believe just over 18 months ago, where in fact only

[Traduction]

nombre des témoins qui ont comparu devant le Comité ont contesté les chiffres qui ont été fournis pour expliquer l'incidence des crimes relatifs aux ordinateurs, et en particulier la théorie de l'iceberg préconisée par M. Parker. Lorsque M. Peter Ward, de la Société Peat, Marwick and Partners est venu comparaître devant le Comité, il a fait état du travail de M. Parker et il a dit:

L'une des citations que j'affectionne le plus à propos du crime informatique est celle qui dit que plus de 85 p. 100 des actes criminels en matière informatique ne sont jamais signalés. La dernière fois que je l'ai entendue, c'était à l'occasion d'un colloque organisé par la Police provinciale de l'Ontario à propos du crime informatique, colloque auquel j'ai assisté avec, pour voisin immédiat, le solliciteur général de cette province. Voilà donc trois extraits qui renforcent ma conviction selon laquelle le crime informatique est devenu une véritable mythologie. Comme dans le cas de la mythologie classique, nous devrions nous attacher à remonter aux sources pour vérifier l'origine. Prenons la dernière citation. Je vais vous lire un extrait d'une lettre de M. Don Parker dont le nom, j'imagine, revient souvent dans les documents que vous avez lus.

Dans mon ouvrage intitulé *Crime by computer*, j'explique ce chiffre de 85 p. 100...

et il dit:

et entre parenthèses, si vous essayez de retrouver l'origine de ce chiffre de 85 p. 100, vous tombez inmanquablement sur le nom de M. Parker.

... en disant qu'il était fondé sur une étude des actes criminels accompagnés de violence signalés à Detroit. Une étude plus récente encore effectuée à Los Angeles arrive à la même conclusion. J'en ai conclu que les cas d'actes criminels perpétrés au niveau des employés de bureau devaient être encore moins nombreux à être signalés. Il est alors très vraisemblable que plus de 85 p. 100 des crimes informatiques soient passés sous silence.

M. Ward poursuit en disant que l'on ne peut peut-être pas dresser une analogie à partir des crimes violents.

Il dit:

Voici des chiffres vérifiables: à l'échelle mondiale, on signale chaque année environ 75 cas d'utilisation abusive des ordinateurs.

J'aimerais d'ailleurs insister sur le terme «signaler». Le nombre de cas ainsi signalés semble également plafonner. Si vous vous reportez aux tableaux publiés tout récemment dans les ouvrages de M. Parker et à ceux que contiennent les documents publiés par le *Stanford Research Institute*, les premières prévisions qui remontaient au milieu des années 70 et qui faisaient état d'une croissance absolument phénoménale du crime informatique ne se sont jamais matérialisées à la fin des années 1970. Ces mêmes données nous montrent que les pertes annuelles moyennes signalées se chiffrent à environ 30 millions de dollars, et il s'agit une fois encore de chiffres valant pour le monde entier.

Enfin, l'inspecteur Campbell, de la Division des escroqueries de la Police provinciale de l'Ontario, a procédé il y a un peu plus d'un an, peut-être 18 mois, je crois, à une

[Text]

2% of the surveyed companies reported any incidence whatever in a very broad definition of computer crime.

What are the facts? To what extent is computer crime a problem, if you take a fairly broad definition of computer crime or computer abuse? Is Mr. Ward correct when he says 75 reported world-wide cases each year, and that it appears to be levelling off as opposed to increasing? Or is there some reason to believe that Mr. Parker's iceberg theory has some validity?

Mrs. Nycum: It is an excellent question you raise. Indeed, in Don Parker's most recent book, of which I just received a copy before I came up, there is a chapter on this point, and it is entitled "How much computer crime is there?". I would refer you to it because he is essentially saying that we do not know, and I think that is the only answer that anyone who is thoughtful can give. We certainly do not know.

• 1625

I remember that, at the very outset of the studies there were numbers bandied about, that is the only way I can say it, saying that only 15% of computer crime had been reported. It just bothered me, logically. How do you get 15% from a number you do not know the size of. I had thought it came from one source, and that person denied it. It is one of those things, I guess. It is like gossip; if you track it down, you will find that no one will own up to it, and everyone looks to someone else but no one has the facts to base it on.

There are a couple of reasons, I think, why no one really does. One of those reasons is that no one agrees on a definition of computer crime, so there will be very narrow definitions and very broad definitions. Those definitions will be arrived at to serve the purpose of the person who is using them. The second thing is that, even if there were a good, agreed to, standard definition, people simply are not required to report crime or abuses to them as victims. It is not the kind of thing people like to stand up and be counted on, particularly, in a business context.

We just simply do not know how much there really is, but I do know that there is some. It does exist, and I do know that it has ramifications on society directly, as in the case of the people who were using the automated teller machines in New York where the Attorney General had to bring an action against Citibank, who had been charging those individual customers for the missing funds.

Two indirect consequences are when a company is bankrupted or somehow computer crime has led, as in other forms of crime, to raising the cost of goods and services. To really answer your question—what is the situation, what is the nature and extent of it—I cannot give you any statistics that would be useful, and I would suggest that anytime anyone does that, you look him very, very strongly in the eye.

[Translation]

enquête qui lui a permis de conclure que sur toutes les compagnies interrogées, 2 p. 100 seulement avaient signalé des cas de ce genre, et encore s'agissait-il d'une définition extrêmement générale du crime informatique.

Quels sont donc les faits? Si vous prenez une définition assez large du crime informatique ou de la truandique, dans quelle mesure cette infraction constitue-t-elle un problème? M. Ward a-t-il raison lorsqu'il dit qu'on signale chaque année 75 cas à l'échelle mondiale et que cela semble plafonner au lieu d'augmenter? Ou alors y a-t-il lieu de croire que la théorie de l'iceberg de M. Parker revêt un certain intérêt?

Mme Nycum: Vous soulevez une excellente question. D'ailleurs, dans le livre le plus récent de Don Parker, dont j'ai reçu un exemplaire juste avant de venir, il y a un chapitre qui traite de cela et qui s'intitule *How much computer crime is there?* Je vous le signale, parce qu'il y dit en gros que nous ne savons pas, et je pense que c'est là la seule réponse que puisse donner une personne réfléchi. Nous ne savons pas du tout.

Je sais que, dès le début des études, des chiffres avaient été brandis, c'est la seule façon de le dire, pour soutenir que 15 p. 100 des crimes informatiques seulement étaient connus. Personnellement, cela ne m'a jamais semblé logique. Comment peut-on calculer 15 p. 100 à partir d'un chiffre qu'on ne connaît pas? Je croyais qu'il y avait une source, mais la personne en question l'avait nié. Vous voyez le genre de choses. C'est comme les commerces, quand vous les retracez, vous constatez que personne n'en accepte la responsabilité, personne ne connaît les faits et tout le monde cite quelqu'un d'autre.

En fait, je pense que cela est dû à deux choses. D'une part, personne n'est d'accord sur une définition du crime informatique, si bien qu'on retrouve des définitions larges et d'autres très étroites. Les gens inventent les définitions qui leur conviennent. En deuxième lieu, même avec une bonne définition reconnue et normalisée, comme les gens ne sont pas tenus de signaler qu'ils ont été victimes de crime ou d'abus, ce n'est pas le genre de choses qu'ils ont tendance à avouer, surtout dans le monde commercial.

En réalité, nous ignorons tout simplement l'ampleur du problème, tout ce que nous savons, c'est qu'il y a un problème. Il existe et je sais qu'il a des effets directement sur la société, dans le cas, par exemple, des gens qui utilisent les guichets de banque automatiques à New York; le procureur général a été forcé d'intenter des poursuites contre Citibank qui faisait payer à ses clients l'argent qui disparaissait.

A cela, deux conséquences indirectes: lorsque certaines formes de crime informatique conduisent une compagnie à la faillite, cela provoque une hausse des prix des biens et des services. Pour répondre à votre question, quelle est la situation, quelle est sa gravité, je ne peux pas vous citer de statistiques utiles et je pense que vous auriez intérêt à regarder bien droit dans les yeux quiconque vous en citerait.

[Texte]

Mr. Beatty: Is anyone systematically compiling statistics, particularly in the U.S. in view of the fact that many jurisdictions now have computer crime statutes on the books.

Mrs. Nycum: Thank you for that question. The bureau of justice statistics in the Department of Justice in the U.S. has a project now, which Don and I are working on, which is to look at the experiences of the jurisdictions which have computer crime laws to see what use has been made of them, and to what extent there has been a feeling that they have been useful. That study is just barely beginning, and so we will not have the results of it for several months, but that is an attempt by the Department of Justice to quantify the experience under those laws.

About 18 months ago, I worked with someone on another project in electronic funds transfer crime where we again tried to quantify the experience for the bureau of justice statistics and found that it was nigh on impossible to get a true picture of what was happening for the reasons that I just discussed.

Mr. Beatty: Some jurisdictions have mandatory reporting clauses in their computer crime statutes. In the work you have done, have you found there to be a major difference in the terms of the incidences reported on computer crime from jurisdiction to jurisdiction on the strength of the mandatory reporting provisions?

Mrs. Nycum: We do not have that data yet. I would say at the federal level a mandatory reporting requirement is being resisted by consumers and people who might be victims.

Mr. Beatty: Certainly, I think most of the testimony we have had before the committee so far has generally been against including mandatory reporting. In some instances, for example, a university, or another institution which would have an employee that would borrow time for joy riding, might feel that internal disciplinary measures were sufficient without having to report to the police. They would resist being forced to do it. It is also the PR aspect, I suppose, as well.

Mrs. Nycum: Yes. And a concept of materiality. When one is a reporting company in the United States under the securities and exchange laws, if the incident is such that there has been a material impact on the company, then there are other reasons why it has to be reported. However, if it is not, then the PR aspect would indeed enter into it. And, indeed, it might be considered to be sensible management not to, just because of the impact on the confidence in the company.

• 1630

Mr. Beatty: Now, when the Canadian Bankers' Association was before the committee, it differentiated between crimes where the computer happened to be involved, but which could be prosecuted in other ways, and crimes where—potential crimes which are not against the law at the present time, where a computer is involved. They really had three categories where they felt you could legitimately categorize computer

[Traduction]

M. Beatty: Est-ce que quelqu'un a entrepris de rassembler systématiquement des statistiques, en particulier aux États-Unis, étant donné qu'il y a beaucoup de juridictions qui ont déjà des lois relatives au crime informatique?

Mme Nycum: Merci d'avoir posé cette question. Le bureau des statistiques de la justice du ministère de la Justice des États-Unis a commencé un projet, dont Don et moi-même nous occupons, qui consiste à rassembler les expériences des juridictions qui ont adopté des lois relatives au crime informatique, pour voir comment ces lois sont utilisées et dans quelles mesures elles sont jugées utiles. Cette étude vient de commencer, il faudra donc attendre des résultats plusieurs mois encore, mais, en tout cas, le ministère de la Justice essaie de quantifier l'expérience de ces lois.

Il y a environ 18 mois, j'ai travaillé sur un autre projet relatif au crime de transfert électronique de fonds; là encore, nous avons essayé de quantifier les expériences du bureau des statistiques de la justice et nous nous sommes aperçus qu'il était pratiquement impossible de nous faire une juste idée de la situation, précisément pour les raisons dont je viens de parler.

M. Beatty: Les statuts relatifs au crime informatique de certaines juridictions obligent les victimes signaler les incidents. Au cours de vos travaux, avez-vous constaté que ces dispositions portant déclaration obligatoire fassent une différence notable quant au nombre des incidents signalés?

Mme Nycum: Nous n'avons pas encore ces données. Je peux vous dire que, dans la mesure où c'est une exigence fédérale, cette obligation de signaler les incidents ne plaît ni aux consommateurs ni aux victimes possibles.

M. Beatty: En tout cas, dans la plupart des témoignages que nous avons entendus jusqu'à présent, les gens sont contre l'obligation de faire rapport. Dans certains cas, prenez une université ou une autre institution dont un employé vole du temps d'ordinateur on considère souvent que des mesures disciplinaires internes sont suffisantes et qu'il est inutile d'en parler à la police. Ils n'aimeraient pas du tout qu'on les force à le faire. Il y a également le problème des relations publiques, j'imagine.

Mme Nycum: Oui. Il y a également l'aspect matériel de la question; supposons qu'on signale un incident dans une compagnie américaine en application des lois sur les valeurs mobilières, si l'incident a des effets matériels sur la compagnie, il y a d'autres raisons d'en faire rapport. Mais même lorsque ce n'est pas le cas, l'aspect relations publiques joue toujours. D'ailleurs, il est fort possible que la compagnie décide de ne pas en parler pour ne pas porter atteinte à sa réputation.

M. Beatty: Lorsque l'Association des banquiers canadiens a comparu devant le Comité, ils ont fait une différence entre les crimes où l'ordinateur jouait un rôle mais qui pouvaient faire l'objet de poursuites grâce à d'autres textes de loi et les crimes—du moins les incidents qui pourraient devenir des crimes mais, pour l'instant, ne sont pas illégaux, et qui mettent en cause un ordinateur. Pour eux, il y a trois catégories de

[Text]

crimes that were not covered by the law at the present time: First, unauthorized access to a computer; second, use of time, and the third, system crashing, I believe.

I asked them whether they had, in any survey of their members, found any instance where there had been unauthorized access to a bank computer in Canada, and they said that they were unaware of a single instance, except where fraud, for example, had taken place. Are you aware of instances in other jurisdictions where, for example, banks that have their systems on line—someone has been able to tap into the system without committing fraud in some way or without committing an offence which is prosecutable under other statutes?

Mrs. Nycum: Yes. In the U.S. we have the wire fraud statute which in most cases is involved in the bank incidents that have occurred, and there is some feeling that that wire fraud statute is broad enough to take care of almost any problem that might arise, particularly when there is a transfer between branches of a bank. In other words, it does not happen just internal to a particular branch of a bank but involves any kind of use of the wires, communications.

Under the Financial Institutions Regulatory Control Act of 1978, we have criminal provisions for the ATM type of abuse. So there is specific legislation on point there.

Mr. Beatty: I would think in any case with an ATM you are dealing with fraud. It matters little whether you give false information to an ATM or to an individual who is a teller. You are committing fraud nonetheless.

Mrs. Nycum: Yes. And some of the other particular types of laws which are in use and have been used for computer and banking perpetrations have been the alteration of bank records, which is a federal crime in the U.S. And almost everything that we have found in the salami techniques and otherwise are of course altering the bank records. So there is an existing network of laws in place in that particular segment. But we had some problems when we got out of the brick and mortar situation and into the—and we are not sure how this is going to work yet, because we do not have experience—home banking, how that is going to be affected. It may or may not fit nicely into some existing laws.

Mr. Beatty: Are you aware of any instance where a person has been able to access a bank's computer to gain credit information, for example, about another individual or where someone was just joy-riding as opposed to attempting to defraud the institution?

Mrs. Nycum: The one that comes to my mind is not a bank for that information but a credit reporting agency, and the research that we did could find absolutely nothing that was wrong with the following scenario: Let us assume that I want to get some credit and I do not have any good credit, so I use yours, and you find out somehow that I have done this. You complain about it and you are asked well, what loss did you

[Translation]

crimes informatiques qui ne sont pas prévus par la loi à l'heure actuelle: premièrement, accès non autorisé à un ordinateur; deuxièmement, utilisation de temps d'ordinateur et, troisièmement, effraction du système, je crois.

Je leur ai demandé si, en consultant leurs membres, ils avaient entendu parler de cas où l'on aurait pénétré sans autorisation dans un ordinateur de banque au Canada; ils m'ont répondu qu'ils n'étaient pas au courant du moindre cas de ce genre, sinon des cas de fraude. Est-ce que vous savez si dans d'autres juridictions, il y a eu des cas d'effraction des systèmes des banques qui n'auraient pas constitué une fraude ou un délit susceptible de poursuite?

Mme Nycum: Oui. Aux États-Unis, il y a un statut sur les fraudes électroniques qui a pu être invoqué dans pratiquement tous les incidents mettant en cause des banques. On pense généralement que ce statut est suffisamment large pour régler les problèmes qui pourraient se poser, surtout les cas de transfert entre les succursales d'une banque. Autrement dit, ce n'est pas une opération interne dans une succursale particulière d'une banque, mais toute communication qui passe par un fil.

Sous le régime de la *Financial Institutions Regulatory Control Act* (Loi sur le contrôle de la réglementation des institutions financières) de 1978, nous avons des dispositions criminelles pour les infractions qui mettent en cause un guichet automatique. Par conséquent, il y a déjà des dispositions spécifiques.

M. Beatty: J'imagine que lorsqu'il s'agit d'un guichet automatique, il y a forcément fraude. Peu importe que vous donniez des informations inexactes à un guichet automatique ou à un être humain qui est caissier. La fraude est la même.

Mme Nycum: Oui. Il y a d'autres lois qui ont été invoquées dans le cas de délits informatiques et bancaires: les lois relatives à la falsification des dossiers bancaires qui est un crime fédéral aux États-Unis. Pratiquement tout ce que nous avons découvert, les techniques *Salami* et autres, sont en réalité la falsification de dossiers bancaires. Il y a donc déjà toute une série de lois dans ce domaine. Mais nous avons eu des problèmes lorsque nous nous sommes écartés des éléments fondamentaux—d'ailleurs, nous ne sommes pas encore certains que cela fonctionne parce que nous n'avons pas d'expérience: nous ne savons pas quels seront les effets des opérations bancaires à domicile. Il est possible que les lois actuelles soient parfaitement suffisantes.

M. Beatty: Connaissez-vous des cas où une personne a pu pénétrer dans un ordinateur de banque pour recueillir des informations relatives au crédit, par exemple, d'une autre personne? Ou encore des cas de frasque, et non de fraude contre l'institution?

Mme Nycum: Le premier cas qui me vient à l'esprit ne met pas en cause une banque mais une compagnie d'enquête sur le crédit, et au cours de nos recherches, nous n'avons pas réussi à trouver la moindre irrégularité dans le scénario suivant: supposons que je souhaite obtenir un crédit mais que mon crédit ne soit pas très bon. Je décide donc d'utiliser le vôtre et, d'une façon ou d'une autre, vous vous en apercevez. Vous vous

[Texte]

suffer. We actually had a case of that sort in which no one could ... There was known to be some sort of at least insult, but no one could find an actionable wrong ...

Mr. Beatty: Was that an impersonation ...

Mrs. Nycum: Yes. In other words, I borrow your identity to get something but you are not injured. I do not cause you any loss at all, but I have borrowed your identity.

• 1635

Mr. Beatty: You may not be able to have a civil remedy, but—I do not know whether Mr. Hill might be able to clarify it for us—I would imagine that under Canadian law that would be impersonation and would be illegal. It would be a criminal offence.

Mrs. Nycum: You are right. It was not in ours.

Mr. Beatty: The key question, I think, for this committee is where are the holes in the law as the law stands today in Canada—and I realize you are at a disadvantage there—which need to be closed. What is the American Congress looking at that is not covered today under various statutes which require that some action be taken to deal expressly with computers?

Mrs. Nycum: The one that I am tremendously aware of I understand is indeed covered in your law. We have no law that neatly covers the transference of electronic impulses from place to place. Not under our federal jurisdiction nor in any of our state jurisdictions does that constitute property. So our federal and our state stolen property statutes do not apply. There is not a thing which is being taken. It also is a problem if the person is looking at the information but has not reduced it to a tangible in some fashion. If I access it by visual terminal and gain knowledge but do not have a thing to take away, in some jurisdictions there is a real loophole.

Mr. Beatty: We have the same loophole here. If I were to gain access to your data base and to browse through it and even to copy the information that was held in there, without depriving you of the original, it appears the law would not cover that. But would you recommend that the law make a differentiation between information that is stored electronically and information that is stored in manual form? Presumably it is not different from if I were to look through your briefcase and copy material you had in it.

Mrs. Nycum: Of course if you made a copy of material in my briefcase, I would not have a problem under U.S. law, because under our theft of trade secrets statutes, in particular ... let us assume what I have is confidential; then there is clearly a thing that I had taken from me. From a civil standpoint in many of our jurisdictions there is not a problem even if you take it away in your head, because you are unfairly

[Traduction]

plaignez et on vous demande quelle perte vous avez subi à la suite de mes actions. En fait, nous avons vraiment eu un cas comme celui-là où personne ne pouvait ... C'était plus ou moins comparable à une insulte mais personne n'a pu trouver un tort ...

M. Beatty: S'agissait-il d'une falsification d'identité ...

Mme Nycum: Oui. Autrement dit, j'emprunte votre identité pour obtenir quelque chose mais, cela ne vous touche pas vraiment. Je ne vous cause aucune perte, mais j'ai tout de même emprunté votre identité.

M. Beatty: Vous n'avez peut-être pas de solution au civil, mais j'imagine que, et M. Hill pourrait peut-être nous éclairer là-dessus, selon le droit canadien, ce serait de l'usurpation d'identité et de ce fait illégal. Ce serait un acte criminel.

Mme Nycum: Vous avez raison. Mais ce n'est pas comme cela chez nous.

M. Beatty: La grande question, je pense, pour le Comité, c'est de savoir où sont les lacunes dans les lois actuellement en vigueur au Canada, et je sais bien que le droit canadien ne vous est pas tellement familier. Quelles mesures qui n'existent pas actuellement dans les diverses lois le Congrès américain envisage-t-il de prendre pour traiter spécifiquement des ordinateurs?

Mme Nycum: Je suis très au courant d'une mesure qui est prévue je pense dans l'une de vos lois. Chez nous, aucune loi ne vise précisément le transfert d'impulsions électroniques d'un endroit à l'autre. Cela n'est considéré comme de la propriété ni par les lois fédérales, ni par les lois d'État. Alors, les dispositions des lois fédérales et d'État concernant le vol de propriétés ne s'appliquent pas. La notion de propriété ne s'applique pas en pareil cas. Il y a un autre problème: si la personne consulte des données sans les recopier d'une façon quelconque, la loi ne s'applique pas. Dans certains États, il y a une véritable lacune en ce sens que la loi ne s'applique pas si quelqu'un a accès à de l'information par la voie d'un terminal, en assimile des données mais n'en apporte rien de concret sous quelque forme que ce soit.

M. Beatty: La même lacune existe ici. Si j'avais accès à votre base de données et que j'y furetais, même si je reproduisais l'information qu'elle renferme, sans vous priver de l'original, il semble que la loi ne s'applique pas à cela. Recommanderiez-vous que la loi établisse une distinction entre l'information emmagasinée électroniquement et l'information classée manuellement? Je présume que ce n'est pas différent que de copier de l'information que je trouverais dans votre serviette.

Mme Nycum: Si vous copiez de l'information à partir de documents pris dans ma serviette, je n'aurais pas de problèmes, puisqu'en vertu du droit américain, des lois sur les secrets industriels en particulier, s'il s'agissait de renseignements confidentiels, par exemple, il serait aisé de prouver que j'ai été victime de vol. Du point de vue du droit civil, dans de nombreux états, même si vous ne faites que mémoriser des données,

[Text]

competing with me by virtue of the information that was mine. But from a criminal standpoint, in some of our jurisdictions, as I say, there is this loophole; and as we go more and more to computers that are CRT-type, or just read-outs rather than print-outs, I see a loophole there.

Mr. Beatty: You are saying that in the U.S., if I understand you correctly, trade secrets legislation would apply to manually held information but not to electronically stored information?

Mrs. Nycum: No. What I am saying is... well, possibly I am saying it, by suggesting that in the U.S. there is this concept of the trade secret being represented in some fashion in a tangible before there can be any taking. A leading jurisdiction in that respect is California. The penal code section is 499(c), and it does require that there be some tangible which is asported before there is a completion of that theft of the trade secret.

Mr. Beatty: In most American jurisdictions that have acted on this, has theft of time been an offence, and would you recommend that theft of time on a computer be included as an offence and changed in our criminal code?

Mrs. Nycum: As you know, in our jurisdictions there is a United States code, which is a federal jurisdiction, and then each state has its own. Some will have a services provision and some will not. There is a theft of government services provision, and that has been used effectively by U.S. attorneys to prosecute theft of computer crime from government installations. But in terms of the numbers of incidents there are of theft of computer time or services, in our experience the numbers have been high enough to warrant a direct approach to making that specifically a criminal act, and I would recommend it, because it has made it difficult for prosecutors when it has been unclear whether they could bring an action or not under theft statutes of a particular state. They would have found it much more helpful to have had something that said directly, yes, computer services, including computer time, would be a crime.

• 1640

Mr. Beatty: There are two or three options that we would have. One would be something analogous to data trespass or computer trespass, unauthorized access to computer. They would say that if you are able to violate the sanctity of the machine you have committed an offence if you were not authorized, irrespective of how much time you use. The mere fact of being there would be analogous to trespass. I suppose if I were to go into your office you would be less worried about the wear and tear on the rug than you would about the fact that I was there. Or you could go a step further and say that there is in fact value in the computer time that you have stolen and that this should be of some importance.

I am inclining toward the belief that we should be looking at unauthorized access rather than time. The cost of time has fallen dramatically. You would find a great deal of variation from institution to institution insofar as they are concerned about the use of time. Also, if you are able to keep somebody

[Translation]

vous contrenez à la loi parce que vous concurrencez injustement avec moi grâce à de l'information qui m'appartenait. Mais du point de vue droit criminel, dans certains états, comme je l'ai dit, cette lacune existe; et plus on fera appel aux écrans plutôt qu'aux imprimés, plus cette lacune s'aggravera.

M. Beatty: Vous dites qu'aux États-Unis, si je vous comprends bien, la Loi sur les secrets industriels s'applique à de l'information classée manuellement mais non à l'information emmagasinée électroniquement?

Mme Nycum: Non. J'ai peut-être donné à entendre que, aux États-Unis, il faut que de l'information se trouve sous forme tangible avant qu'il y ait infraction aux termes de la Loi sur les secrets industriels. La Californie est un bon exemple d'un état qui applique ce principe. Selon l'article 499(c) du Code pénal, il faut que l'information se trouve sous forme tangible quelconque avant qu'on puisse considérer qu'il y a eu vol d'un secret industriel.

M. Beatty: Dans la plupart des états américains qui ont pris des mesures dans ce domaine, le vol de temps d'utilisation d'un ordinateur constitue-t-il une infraction, et recommanderiez-vous qu'une telle infraction soit prévue dans le Code criminel?

Mme Nycum: Comme vous le savez, chez nous, il y a un code pénal américain, qui est du ressort fédéral, et puis un code pénal pour chaque état. Certains prévoient des dispositions concernant les services, d'autres non. Il existe une disposition concernant le vol de services gouvernementaux, et les procureurs américains y ont fait appel avec succès pour des poursuites pour vol de temps d'utilisation d'un ordinateur du gouvernement. La fréquence de vols de temps d'utilisation ou de services d'ordinateurs est suffisamment importante, et le nombre d'infractions suffisamment élevé pour justifier que cela devienne un acte criminel, et je ferais une recommandation en ce sens, parce que les procureurs ont eu de la difficulté à déterminer si des poursuites pouvaient être intentées en vertu des lois concernant le vol de certains états. Il aurait été beaucoup plus facile d'établir explicitement que les services d'ordinateurs, y compris le temps d'utilisation constituaient un crime.

M. Beatty: Nous avons trois options. La première serait quelque chose d'analogue à la violation d'information ou d'ordinateur, soit l'accès non autorisée à un ordinateur. Le fait d'utiliser un ordinateur sans autorisation constituerait une infraction, peu importe le temps d'utilisation. Cela correspondrait à une violation. Si je pénétrais dans votre bureau, je suppose que vous vous inquiéteriez moins de l'usure de votre tapis que du fait que je sois là. Ou, vous pourriez aller un peu plus loin et dire que le temps pendant lequel vous avez utilisé l'ordinateur a effectivement une valeur et qu'on doit y accorder une certaine importance.

Mais je suis porté à croire que nous devrions insister sur l'accès non autorisé plutôt que sur le temps d'utilisation. Le coût du temps d'utilisation a baissé considérablement. Vous constateriez énormément de différence quant à l'importance que chaque institution accorde au temps d'utilisation de son

[Texte]

from getting in the door in the first place, you have pretty well solved the rest of the problems.

Mrs. Nycum: We have a problem in the United States with a number of jurisdictions which have used the expression "unauthorized access" and made it a crime to commit an unauthorized access. What is unauthorized has been the problem. From computer installation to computer installation, sometimes within the same organization or company, there has been a difference in what is authorized and what is unauthorized. Then you have the question of if you are authorized to get on the system to do one thing and indeed once you are there do something else, have you then gone... It is just like saying you may come into the public area of the building but not into the inner chambers. That has been pointed out as a flaw in some of the thinking behind some of our legislation.

Mr. Beatty: Could you expand on that? I think the analogy of trespass is a useful one. When I met you at security down at the front here, I thought about when I visited Washington. Security there is very different, say in the State Department, where you appear to be able to walk in, but you meet security on every floor, depending on the specific area that you are going into and how confidential the work being done there is. It is easy to get into the premises in the first place, but depending on where you go from there there are different levels of security. Presumably the principle they would follow is that you may be authorized to penetrate the system or the building to a certain level but there are other areas where you cannot go. Presumably in trespass you would have something similar to that.

What legal problems does this pose? Is there not a computer analogy that one can build from that?

Mrs. Nycum: You are assuming now that the things are all going to be done by outsiders, and the people who work in the computing industry are concerned because sometimes an access is authorized and sometimes it is not. It depends on the management of the facility to determine what is authorized and what is not authorized, and, candidly, in many cases we found there has not been a policy at all.

Mr. Beatty: But that is the fault of management, then. I suppose the classic case is where there is time-sharing. You are authorized to get in to use the computer for the purposes for which you contracted; you are not entitled to get into your neighbour's portion of the data base, which deals with your neighbour's records. The same thing applies if you are in a building like a hotel. You are surely entitled to come into the lobby, but you are not necessarily entitled to go through the offices.

Mrs. Nycum: That works quite neatly for outsiders, who have to assume that they are not invited into any part unless the invitation has been extended, or there is a sign that says this is not for you, if it appears to be a public building. The concern among the people in the computing business in the United States has been where there is an authorized use for some people but not all people who are in the organization. Sometimes any use has been encouraged and other times very

[Traduction]

ordinateur. De plus, si vous réussissez à interdire l'accès des lieux aux intrus, les autres problèmes risquent de ne même pas se produire.

Mme Nycum: Nous avons un problème aux États-Unis avec un certain nombre d'États qui ont utilisé l'expression «accès non autorisé» et qui ont fait de cet acte un acte criminel. Le problème réside dans ce qu'on entend par autorisé ou non autorisé. Les interprétations varient d'un service informatique à l'autre, et parfois au sein de la même organisation ou compagnie. Ensuite, il y a la question de savoir si vous êtes autorisé à utiliser le système pour effectuer une tâche et que vous l'utilisez à d'autres fins, si vous ne contrevenez pas alors... C'est comme permettre à quelqu'un de circuler dans les endroits publics d'un édifice, mais pas dans les bureaux intérieurs. C'est une lacune de certaines de nos lois qu'on a fait ressortir.

M. Beatty: J'aimerais approfondir cette question. Je pense que l'analogie de la violation est utile. Quand je vous ai rencontré en bas au bureau de la sécurité, à l'entrée, j'ai pensé à ma visite à Washington. La sécurité là-bas est très différente, disons dans un ministère d'État, où il semble facile d'entrer, mais il y a des contrôles de sécurité à chaque étage, selon le service dans lequel vous vous trouvez et le caractère confidentiel du travail qu'on y effectue. Il est facile de pénétrer les lieux, mais selon l'endroit où vous allez à partir de l'entrée, les niveaux de sécurité sont différents. Le principe est probablement que vous pouvez être autorisé à pénétrer le système ou l'édifice jusqu'à un certain point, mais qu'il y a d'autres secteurs où vous n'êtes pas autorisé à entrer. La même chose pourrait peut-être s'appliquer au principe de violation.

Quels problèmes légaux cela poserait-il? N'y a-t-il pas une analogie à créer à partir de cela qui s'appliquerait à l'ordinateur?

Mme Nycum: Vous prenez pour hypothèse que les infractions seront perpétrées par des gens de l'extérieur, et que les personnes travaillant dans l'industrie de l'informatique se préoccupent de la question de savoir si l'accès est autorisé ou non. Cela dépend de la politique de gestion, et dans bien des cas, nous avons constaté l'absence complète de politiques concernant l'accès au service.

M. Beatty: Mais c'est la direction qui est à blâmer dans cela. Je suppose que le problème typique est celui du système à utilisateurs multiple. Vous êtes autorisé à utiliser l'ordinateur à des fins bien précises; vous n'avez pas le droit d'empiéter sur la base de données de votre voisin qui porte sur les dossiers de votre voisin. La même chose s'applique si vous êtes dans un édifice comme un hôtel. Vous avez sûrement le droit de circuler dans l'entrée, mais vous n'avez pas nécessairement le droit d'entrer dans les bureaux.

Mme Nycum: Cela fonctionne assez bien pour les gens de l'extérieur qui doivent considérer qu'ils n'ont pas le droit d'entrer quelque part sans qu'ils y soient invités expressément, ou qui doivent respecter les affiches leur interdisant l'accès à certains lieux, s'il s'agit d'un édifice public. Le problème de certaines personnes du milieu de l'informatique aux États-Unis tient au fait qu'au sein de la même organisation, certains peuvent être autorisés à utiliser des installations alors que

[Text]

strictly not. Where we have got some of those questions—that is, what is an authorized use of the computer and hence the access for that purpose—the joy-riding and the Snoopy calendars, that sort of thing, have really got them very, very concerned, because the penalties for unauthorized use, and hence access, have been set quite high. So I am commenting not on the legality, not on the legal analysis here, but on the perception of the people who look at these laws and say, how does that apply to me.

[Translation]

d'autres ne le sont pas. Parfois on encourage une utilisation presque illimitée d'installations, alors que d'autres fois, l'accès y est très limité. Chaque fois que l'une de ces questions se pose, par exemple qu'est-ce qui constitue une utilisation illicite de l'ordinateur et, partant, le branchement effectué à cette fin, le resquillage et les calendriers Snoopy, j'en passe, tout cela donc les inquiète beaucoup en raison des peines qui frappent toutes ces utilisations illicites, de même que les branchements illicites, lesquels sont très sévères. Je ne fais donc pas ici de l'analyse juridique, mais je me place du point de vue de ces gens qui lisent la loi et qui se demandent à quel point elle s'applique à eux.

• 1645

Mr. Beatty: One final question, because my colleague has been very patient, and I have gone on at some length. Could you comment on the possibility of including data security standards in the law? To what extent should the institution that holds information be held responsible under the law for the security of that information? In particular, if lax security results in losses to the institution or in a third party's being damaged—for example, through an invasion of your privacy, if your credit records or medical records were held in an institution's computer... should there be some criminal liability on the part of the institution if their standards are not high enough? Should there be some civil recourse open to you? If in fact it is necessary to impose security standards on institutions, what mechanism would you envisage for doing that? You would imagine that the degree of security would vary from institution to institution on the strength of the information being held in the computer. How could the government establish these standards and how could it enforce them?

M. Beatty: Une dernière question si vous voulez bien parce que mon collègue s'est déjà montré extrêmement patient et je sais que j'ai été très long. Que diriez-vous de la solution qui consisterait à intégrer à la loi certaines normes sur la protection des données? Dans quelle mesure l'organisme qui détient ces données devrait être considéré aux yeux de la loi comme responsable de la protection de ces mêmes données? Je pense notamment au cas d'une carence au niveau de la sécurité qui se traduirait par certaines fuites au détriment de l'organisme ou d'une tierce partie, on peut par exemple imaginer une violation de notre vie privée en cas de piratage d'un ordinateur qui aurait en mémoire vos dossiers médicaux ou votre dossier de crédit, si les normes de l'organisme en question ne sont pas suffisamment draconiennes, ne pourrait-on pas considérer celui-ci comme directement responsable aux yeux du Code criminel? Ne devrait-il pas y avoir certains recours devant les tribunaux civils? Si effectivement on en arrive à devoir imposer aux organismes des normes de sécurité, quel dispositif envisageriez-vous? Evidemment, vous serez d'accord avec moi pour dire que le degré de sécurité varierait d'un organisme à l'autre en fonction de la nature des données ainsi mises en mémoire. Mais comment le gouvernement pourrait-il élaborer ces normes et les faire respecter?

Mrs. Nycum: I think one of the keys to that discussion is just to identify security and what is an appropriate level of security. It happens that for the Department of Justice we did a study on baseline security concepts, and that is a published document that the U.S. Department of Justice has. To my knowledge, it was the first time there had been any baseline—these are the foundations that, we can all agree, should be undertaken. Apart from that, there is no generally accepted body of security techniques such that one could say, yes, if you do not have those you were guilty of negligence, responsible for negligence—let alone guilty of being—what?—an aider, or an abettor, or an accessory, or some such concept under the criminal law. So that would be difficult.

Mme Nycum: Je pense que l'un des éléments essentiels est ici la définition de la sécurité et du niveau de sécurité nécessaire et suffisant. Au ministère de la Justice par exemple, nous avons procédé à une étude sur les notions de sécurité fondamentale, et cette étude a d'ailleurs été publiée par ce même ministère. À ma connaissance, c'était la première fois que ces normes fondamentales pourrions-nous dire avaient été établies et nous sommes tous d'accord pour convenir qu'il importe de fonder tout le système sur ces dernières. Outre cela, il n'existe aucun ensemble communément accepté de méthodes de protection qui nous permettrait effectivement de dire aux organismes que s'ils ne respectent pas ces méthodes, ils se rendent coupables de négligence, ou du moins ils sont responsables sans parler nécessairement de la notion de culpabilité, dans la mesure où ils se rendent d'une façon ou d'une autre complices d'une infraction tombant sous le coup du Code criminel. Il serait donc difficile de tabler là-dessus.

But addressed in the positive way, if you consider that we are looking at something like a concept of computer information as being, say, a trade secret, under U.S. law in order to have a trade secret you have to keep it secret. If the person

Si toutefois on envisage les choses sous un angle positif, si nous reconnaissons que ce qui nous occupe c'est un peu la notion selon laquelle les données informatiques correspondent mettent à un secret commercial, il faut se souvenir qu'aux

[Texte]

failed to keep it secret, by not having security precautions that could be set out in a court proceeding as yes or no, he did that or he did not, then you could proceed to see whether or not the person who perpetrated this had actually stolen a trade secret. In a case I know of in the U.S.—in several of them—there was a lot of evidence as to whether or not there was a trade secret, whether it had been indeed protected.

Mr. Beatty: Thank you very much for a very helpful presentation.

The Chairman: Thank you, Mr. Beatty.

Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Thank you.

At the outset I would like to thank Mrs. Nycum for appearing before the committee and giving us a lot of very useful and helpful information. I am sure it will be of great assistance to us in our deliberations before we write our report.

I noted, Mrs. Nycum, that you amplified in effect, to some extent, parts of the testimony that you gave before the House of Representatives Subcommittee of the Judiciary Committee on Constitutional and Civil Rights. We have a copy of that statement before us and I wanted to ask you several questions about it. Maybe, if you have yours handy, you could refer to it.

Mrs. Nycum: Yes.

Mr. Robinson (Etobicoke—Lakeshore): On page 2 of that report, under the heading, "The Changing Nature of Business and White-Collar Crime", you indicate that in this:

information age, business and white-collar crime is changing significantly. Valuable assets are increasingly represented by information, an intangible property, and its processing, transmission, and storage are rapidly becoming the targets of crime.

Then you go to say:

Such crime includes fraud, theft, embezzlement, larceny, sabotage, espionage, extortion, and conspiracy.

Is this considered to be an exhaustive list? Are there any other areas that you feel properly could be added to this list?

Mrs. Nycum: I am just refreshing my recollection by looking at the list.

• 1650

It is hard to think of any just at the moment. At the time we were attempting just to set out a non-inclusive but representative list of crimes that might be involved.

[Traduction]

termes de la législation américaine, il ne peut y avoir secret commercial que si son détenteur protège ce secret. Si le détenteur ne protège pas le secret, s'il ne prend pas les mesures de sécurité nécessaires qui pourraient être invoquées devant un tribunal, à ce moment-là la question qui se pose est celle de savoir si celui qui a perpétré l'infraction a effectivement volé un secret commercial. Il y a eu aux États-Unis plusieurs causes dont j'ai eu connaissance et au cours des auditions énormément de pièces ont été présentées précisément à l'appui de cette notion de secret commercial et du fait qu'il avait ou non été suffisamment protégé.

M. Beatty: Je vous remercie beaucoup, vous nous avez beaucoup aidés.

Le président: Merci monsieur Beatty.

Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Je vous remercie.

J'aimerais pour commencer remercier M^{me} Nycum d'avoir accepté de comparaître devant nous et de nous avoir énormément aidés comme elle l'a fait. Tout ce qu'elle nous a dit va nous être, je n'en doute pas, extrêmement précieux lorsque nous aurons à rédiger notre rapport.

J'ai relevé, madame Nycum, que vous aviez dans une certaine mesure repris en plus de détails certaines parties de votre déposition devant le sous-comité du Comité judiciaire des affaires constitutionnelles et des droits civiques de la Chambre américaine des représentants. Nous avons reçu copie de votre exposé et je voulais vous poser quelques questions à ce sujet. Si vous en avez vous-même un exemplaire, vous pourriez peut-être nous y renvoyer.

Mme Nycum: Certainement.

M. Robinson (Etobicoke—Lakeshore): A la page 2 du rapport, à la rubrique intitulée «Nouvelle facette de la criminalité à caractère commercial et professionnel», vous dites ceci:

A l'époque de l'informatique, le crime à caractère commercial et professionnel connaît une évolution considérable. De plus en plus, l'information, un bien intangible, acquiert de la valeur et les opérations de traitement, de transmission et de mise en mémoire de l'information deviennent de plus en plus la cible d'activités criminelles.

Et vous poursuivez en disant:

Ces activités criminelles sont par exemple la fraude, le vol, l'escroquerie, le détournement de fonds, le vol simple et qualifié, le sabotage, l'espionnage, l'extorsion et le complot.

Peut-on considérer que cette liste soit exhaustive? Y aurait-il à vos yeux d'autres domaines susceptibles d'y être ajoutés?

Mme Nycum: Laissez-moi me rafraîchir la mémoire.

De but en blanc, c'est un peu difficile. Je pourrais toutefois vous dire qu'à l'époque, nous avions essayé d'établir une liste type mais pas nécessairement complète des actes criminels pouvant être perpétrés.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): When you look at this list of crimes you have enunciated, would these be considered as matters for consideration by state law or would they also be considered as matters for consideration by federal law, in the United States?

Mrs. Nycum: Some would be. Particularly, some would be both and some would not necessarily lend themselves terribly well. For example, there are federal enclaves which for the purposes of jurisdiction are just the same as the state. In other words, everything that happens in the federal enclave is governed by federal law, so you have to have all the types of things that can happen in the federal enclave. In other things that go in, it is not so clear. For example, there is a federal criminal statute directed to theft of trade secrets at the government level where there is theft of someone's trade secret, but it is not the same kind of theft of trade secret as we have at the state level, when you look at it very closely.

So in some respects they are similar and in some respects they are different. I can see that sabotage, for example, or espionage, would be something very important at the federal level, possibly less so at a state level; in particular in certain states.

Mr. Robinson (Etobicoke—Lakeshore): You come from California yourself, and practice there, I assume.

Mrs. Nycum: That is right.

Mr. Robinson (Etobicoke—Lakeshore): Are you satisfied with the California state law or penal code insofar as computer abuse or computer crime is concerned?

Mrs. Nycum: We have a computer crime law in California.

Mr. Robinson (Etobicoke—Lakeshore): I notice in the California penal code there is a definition section, 502, and the definition section defines "access to computer systems", "computer networks", "computer programming data", "financial instrument", "property", which I was surprised would be defined, and other things; but there is no definition of "computer abuse" in this definitive section. Is that an oversight? Is this something that should be amended? Or do you feel it is adequately covered by the statute the way it is?

Mrs. Nycum: The term "computer abuse" we simply coined to take into account the things we wanted to address in our problem domain. We realize that some of these things, like intimidation by computer, might or might not rise to the level of a crime, but we felt they were somehow misuses of computers.

Mr. Robinson (Etobicoke—Lakeshore): You have not identified by way of definition "computer crime" either. You talk about intentional access, or causing to be accessed any computer system or computers, and malicious access, and alterations, deletions, damaging, and so on; but nowhere can I

[Translation]

M. Robinson (Etobicoke—Lakeshore): À en juger d'après cette liste, tous ces actes criminels pourraient-ils être considérés comme tels par les lois des États ou relèveraient-ils également de la Loi fédérale américaine?

Mme Nycum: Certains oui, d'autres non. Certains d'entre eux relèveraient à la fois des deux mais d'autres ne s'y prêteraient pas vraiment. Si, il existe certaines enclaves fédérales qui épousent assez étroitement celles des États. En d'autres termes, tout ce qui se produit dans l'enclave fédérale tombe sous le coup de la loi fédérale, et il faut donc tenir compte de tous les éléments susceptibles de se produire à cet endroit-là. Dans les autres cas, les choses sont moins claires. Ainsi, nous avons une loi pénale fédérale portant sur le vol de secrets commerciaux au détriment du gouvernement, c'est-à-dire les cas de vols de secrets commerciaux appartenant à des tiers, mais cette disposition ne ressemble pas du tout à celle qu'on retrouve dans les lois des États, du moins si on les examine de près.

A certains égards donc, il y a des ressemblances et à d'autres des différences. Ainsi, le sabotage ou l'espionnage sont deux éléments très importants au niveau fédéral mais ils le sont peut-être moins au niveau de l'État, et en particulier dans le cas de certains États.

M. Robinson (Etobicoke—Lakeshore): Vous venez vous-même de la Californie et vous y exercez j'imagine.

Mme Nycum: C'est exact.

M. Robinson (Etobicoke—Lakeshore): Si nous parlons d'utilisation abusive ou illicite de l'ordinateur ou du crime informatique, la législation californienne est-elle à vos yeux suffisante?

Mme Nycum: Nous avons effectivement en Californie une législation punissant le crime informatique.

M. Robinson (Etobicoke—Lakeshore): Je relève dans le Code pénal californien, à l'article 502, une série de définitions notamment des notions «branchement à des systèmes informatiques», «réseaux informatisés», «données à programmation informatique», «instrument financier», «propriété», une définition que je n'aurais pas pensé y trouver, et bien d'autres encore. Toutefois, je n'y remarque aucune définition de l'utilisation abusive de l'ordinateur. Est-ce un oubli? Faudrait-il à vos yeux modifier cet article ou suffit-il à votre avis?

Mme Nycum: La notion d'«utilisation abusive de l'ordinateur» a été forgée pour couvrir les éléments que nous voulions aborder dans ce secteur à problèmes. Nous comprenons fort bien que certains de ces éléments comme l'intimidation par ordinateur pourrait ou non dégénérer en crime, mais nous sommes partis du principe qu'il s'agissait néanmoins d'utilisation illicite des ordinateurs.

M. Robinson (Etobicoke—Lakeshore): Vous n'avez d'ailleurs pas non plus défini ce qu'on pourrait appeler le «crime informatique», la truandique. Vous parlez de branchements délibérés, vous parlez d'actes débouchant sur le branchement à un système informatique ou à un ordinateur, vous parlez de branchement à caractère délictueux, vous parlez

[Texte]

find the term "computer crime" or anything that could be reasonably considered as defining "computer crime".

Mrs. Nycum: The short title of that section is "Computer Crime". The section itself is in the penal code, which is our criminal code in California. Its shorthand term is the "Computer Crime Statute". It addresses wrongful acts having to do with computer systems, computer networks, computer programs, and such.

We do not publish our legislative history in California, unhappily, but the intention was to address what was felt to be the need for a computer crime law. Interestingly, some new bills have been introduced which have not succeeded, which attempt to make some further changes, particularly to the evidence code and so forth.

Mr. Robinson (Etobicoke—Lakeshore): In the absence of having a definitive definition of either "computer abuse" or "computer crime", would you say that one is an extension of the other?

Mrs. Nycum: I would say that computer abuse is things which could be wrongful acts, whether they are simply unethical or they are civil wrongs or they may be criminal acts. The crime then would be, in most jurisdictions, the statutory crime of a particular nature.

• 1655

Mr. Robinson (Etobicoke—Lakeshore): In your view and with your definition, whatever that may be, of computer abuse, do you consider that to be a crime? Is an abuse a crime?

Mrs. Nycum: No, not always.

Mr. Robinson (Etobicoke—Lakeshore): Not always. Well, can you tell me this: when does abuse cease to be abuse and become a crime? Can you draw a line of distinction? Where is the dividing line between one and the other? Or is there a grey area here where somebody has to make a judgment because of the lack of definition?

Mrs. Nycum: I may be taking a very narrow view of this, but the way I look at it is that it is a crime if the legislature or a particular court has found it to be one.

Mr. Robinson (Etobicoke—Lakeshore): That gets us back to the American situation, I suppose, where they say let us go to court and find out.

Mrs. Nycum: In some respects that is the way it is. For example, there are people who are waiting to see, under these new statutes, what the experience will be. I have the feeling that some of them are a little timid to use them because they are afraid they will be challenged, and it will be found that a particular act is not a crime.

[Traduction]

de modifications, de suppressions, de dommages et ainsi de suite, mais vous ne définissez nulle part la notion de «crime informatique» du moins d'une façon qui puisse être jugée satisfaisante.

Mme Nycum: Le titre abrégé de toute cette partie est «crime informatique». L'article proprement dit figure dans le Code pénal qui est l'équivalent de votre Code criminel. L'expression abrégée est «Loi sur le crime informatique» et cette disposition couvre tous les agissements délictueux gravitant autour des systèmes informatiques, des réseaux informatiques, des programmes informatiques et ainsi de suite.

Malheureusement, en Californie nous ne publions pas nos antécédents législatifs, mais nous voulions à l'origine répondre à ce que nous percevions comme un certain besoin, en l'occurrence établir une législation sur le crime informatique. Il est intéressant d'ailleurs de constater que certains nouveaux projets de loi ont été déposés sans guère de succès dans le but précisément de modifier ces dispositions existantes, notamment pour ce qui a trait à la preuve.

M. Robinson (Etobicoke—Lakeshore): À défaut de la définition péremptoire de l'«utilisation abusive de l'ordinateur» ou du «crime informatique», ne diriez-vous pas que l'un est le prolongement de l'autre?

Mme Nycum: Je dirais personnellement que l'utilisation abusive de l'ordinateur représente tous les agissements à caractère délictueux, qu'il s'agisse simplement de manquement à l'éthique ou encore de délits à caractère civil, voire criminel. Dans la plupart des juridictions, le crime s'entendrait du crime statuaire répondant à une définition précise.

M. Robinson (Etobicoke—Lakeshore): A votre avis et compte tenu de votre définition, quelle qu'elle soit, de l'utilisation abusive de l'ordinateur, est-ce pour vous un crime? L'utilisation abusive est-elle un crime?

Mme Nycum: Pas toujours.

M. Robinson (Etobicoke—Lakeshore): Pas toujours. À ce moment-là, quand une utilisation abusive cesse-t-elle d'être une simple utilisation abusive pour devenir un crime? Où est la ligne de démarcation? Y en a-t-il une ou s'agit-il simplement d'une zone incertaine où quelqu'un doit trancher dans chaque cas en raison précisément de l'absence de définition?

Mme Nycum: Peut-être s'agit-il d'une interprétation très étroite des choses, mais pour moi il s'agit d'un crime à partir du moment où l'assemblée ou un tribunal en a décidé ainsi.

M. Robinson (Etobicoke—Lakeshore): Ce qui nous ramène j'imagine au contexte américain où l'on parle du principe qu'il faut demander aux tribunaux de trancher.

Mme Nycum: J'imagine qu'il en est ainsi à certains égards. Par exemple, certains préfèrent attendre les décisions des tribunaux aux termes des nouvelles lois. J'ai pour ma part le sentiment que certains d'entre eux sont un peu timides et hésitent à y recourir de peur de voir leur position contestée, de peur que les tribunaux décident que tel ou tel acte n'est pas un crime.

[Text]

Mr. Robinson (Etobicoke—Lakeshore): Is this one of the areas where you feel that we need to have judge-made law rather than statute-made law?

Mrs. Nycum: In our country even statute-made law is interpreted by the judges. And every time a statute is passed, no matter whether it is civil or criminal, people wait to see how the courts are going to interpret it.

Mr. Robinson (Etobicoke—Lakeshore): Turning to something else, I noticed on page 4 of this statement which you have previously given you talk about a new kind of computer criminal—the “system hacker”. Could you explain a bit more how this works? Is this just related to the individual who is not really proficient at what he is doing; he just happens to come upon a break-in of the computer system or the data-bank? Or when you say a “system hacker”, is he a person who spends all his time trying to break into the system?

Mrs. Nycum: It is closer to the latter definition. I first heard that 10 years ago and wondered what it was. It was a term applied to people who spent more time around computers than they were actually required to. They did it as a hobby, spending most of their lives involved in computing, and not for responsibility, just for fun. They were amateurs rather than professionals.

Mr. Robinson (Etobicoke—Lakeshore): The statement has been made by other witnesses we have had before the committee to the effect that some manufacturers estimate that two out of three of the copies of their product in use have not been paid for. But they do not seem to be too worried about this, because they are making such fantastic profits anyway that I guess they are satisfied without getting the profit on the extra two they are losing.

But it seems to me that police forces should be able to identify the manufacturers, the distributors, the marketers of these copied products. Surely they could be taking action. Why is something not being done?

Mrs. Nycum: That is an excellent question. I think it has to do with the type of copying that is going on. If it were pirating in the sense that records are pirated, I think it would be simpler to identify, because it would be an organized group of people whom one could track down. But it seems that a great deal of this is done by piracy clubs, individuals who trade with each other copies of programs. This includes their parents, who do not seem to think that is a wrong thing to do, although they would be outraged if anyone accused them of stealing. They do not see it as that. So it is not necessarily an organized group of people who are systematically doing it; rather, it is just an awful lot of small incidents.

When I have had an experience with a vendor who feels himself to be in this situation and we have called the public authorities, we have been asked for the proof of our loss. We can say, well, in Los Angeles we know of two, and then there

[Translation]

M. Robinson (Etobicoke—Lakeshore): Pensez-vous qu'il s'agit là justement d'un de ces domaines où la jurisprudence doit l'emporter sur la codification législative?

Mme. Nycum: Chez nous, même les lois sont interprétées par les juges et chaque fois qu'une loi est adoptée, qu'il s'agisse d'une loi à caractère civil ou criminel, les gens préfèrent attendre que les tribunaux en ait fait une interprétation.

M. Robinson (Etobicoke—Lakeshore): Pour passer à un autre sujet, je relève à la page 4 de votre exposé antérieur que vous parlez d'un criminel de l'informatique, d'un modèle nouveau, que vous appelez les casseurs de système. Pourriez-vous nous expliquer ce dont il s'agit? S'agit-il simplement d'un amateur, de quelqu'un qui par hasard arrive à se brancher sur un système ou violer une mémoire ou plutôt de quelqu'un qui a pour principale occupation de forcer les systèmes?

Mme Nycum: Il s'agirait plutôt du deuxième cas. C'est une expression que j'ai entendue pour la première fois il y a une dizaine d'années et à l'époque, je me demandais ce qu'elle voulait dire. On l'appliquait aux gens qui passaient beaucoup plus de temps autour des ordinateurs qu'ils n'étaient supposés le faire. Pour eux, c'était une passe-temps, l'ordinateur les intéressait même si ce n'était pas leur occupation professionnelle, c'était un amusement. C'était donc des amateurs plutôt que des professionnels.

M. Robinson (Etobicoke—Lakeshore): D'autres témoins que nous avons entendus nous ont déclaré que, selon certains fabricants, pour chaque élément de leur production utilisée, il y en a deux ou trois qui ont été copiés. Toutefois, ils ne semblent guère s'en inquiéter étant donné qu'ils font déjà des bénéfices tellement considérables qu'ils s'en contentent sans se préoccuper des pertes qu'ils peuvent subir ailleurs.

Il n'en reste pas moins que pour moi les corps policiers devraient pouvoir être en mesure de mettre le doigt sur les fabricants, les distributeurs et les vendeurs de ces équipements piratés. Il est certain que des mesures pourraient être prises. Pourquoi n'est-ce pas le cas?

Mme Nycum: C'est une excellente question qui porte j'imagine sur le genre de plagiat. Supposons qu'il s'agisse d'un plagiat comparable aux productions pirates de disques phonographiques, la réponse serait simple dans la mesure où on pourrait toujours remonter à la source, c'est-à-dire à un groupe bien organisé. Mais apparemment, il s'agit en l'occurrence ici le plus souvent du fait de petits clubs de pirates, de certaines personnes qui s'échangent les programmes qu'ils ont copiés. Il peut s'agir également des parents qui ne savent peut-être pas que ce n'est pas bien et qui seraient vexés à mort si on les accusait de vol. Pour eux, ce n'est pas du vol. Il ne s'agit donc pas nécessairement d'un groupe organisé qui procède de façon systématique, mais bien d'une foule de petits incidents isolés.

J'ai connu moi-même un cas de ce genre, c'était un revendeur, nous l'avions poursuivi et on nous avait demandé de faire la preuve de nos pertes. Nous pouvons toujours affirmer que nous en connaissons deux à Los Angeles, qu'il y en a eu trois

[Texte]

were three in Florida, and we just have a feeling that there is a lot of this and we are losing a lot. So the public authorities say, well, what is the value of those two in Los Angeles? Oh, \$500? And they essentially are uninterested in the individual loss. So you can see that if we had called up and said there are 50,000 of these in Los Angeles, as an organized event, then we would have had a much better experience, I think, in tracking them down.

• 1700

Mr. Robinson (Etobicoke—Lakeshore): I suppose, since the federal law and the issue are not in being, and many states do not have any laws covering computer access or computer crime, computer abuse, and such, the general public take it for granted that they really have a right to copy if they wish to, because there is no law which says that they cannot do that.

Mrs. Nycum: I think they do not consider it tremendously bad to do it, even though I think in their hearts they know they are doing something wrong. Our copyright law—and most of these mass-produced programs are covered by copyright—permits one copy to be made by the rightful owner of the program. And so, right there, they can see themselves as having the chance to make one copy.

Mr. Robinson (Etobicoke—Lakeshore): So you say it is a matter of morality more than legality. There is no law against it, but morally they should not be making copies; they should not be depriving the . . .

Mrs. Nycum: Well, technically I believe they are violating the copyright law, which is a federal statute, when they make these copies. I do not think there is a concept of fair use there which would permit them to get out from under those sanctions. But they are not actively pursued for a number of different reasons, including the cost of pursuing them, and so they continue. It is regarded as a problem; there is no question about that. It is seriously regarded as a problem.

Mr. Robinson (Etobicoke—Lakeshore): You have a statement to the effect that more money is probably lost from all errors and omissions in the use of computers than is likely lost in all intentional acts. I find that an incredible statement, really. Are people so inept and incapable in using data processing and computers and so on that they are making so many errors and omissions that the loss is even greater? And if they are, would it be fair to suggest that this is a budgetary item? You state that you do not budget for fraud, but certainly you would budget for errors and omissions.

Mrs. Nycum: To the first point, I think we would have to agree with the critics of those who say that computer crime is not particularly a problem; that in comparison to the losses

[Traduction]

en Floride et que nous avons le sentiment qu'il y en a bien d'autres et que nos pertes sont considérables, mais à ce moment-là les pouvoirs publics nous demandent de chiffrer nos pertes et sont tout étonnés lorsque nous leur répondons \$500. Ce qui se passe, c'est que les cas de perte isolée ne les intéressent pas. Bien sûr, si on leur disait qu'il y a 50,000 cas de ce genre à Los Angeles, qu'il s'agit d'un véritable réseau, à ce moment-là nous aurions un dossier plus solide et nous pourrions plus facilement retracer les coupables.

M. Robinson (Etobicoke—Lakeshore): J'imagine donc que, à défaut de loi fédérale et de définition du problème, et vu le fait que de nombreux États n'ont pas encore de législation sur les branchements abusifs ou sur le crime informatique, sur l'utilisation abusive des ordinateurs, la population prend pour acquis que tout le monde a finalement le droit de copier n'importe quoi puisqu'il n'y a aucune loi punissant la chose.

Mme Nycum: Je pense que la plupart des gens ne considèrent pas que ce soit répréhensible même si je suis persuadé qu'ils savent pertinemment bien au fond d'eux-mêmes qu'ils agissent mal. Notre législation sur le droit d'auteur, et j'ajoute que la plupart des programmes produits en série sont protégés par le droit d'auteur, permet à chaque détenteur légitime du programme de faire une copie. Tous ces gens donc considèrent dès lors qu'ils peuvent légitimement faire une copie.

M. Robinson (Etobicoke—Lakeshore): Pour vous donc c'est davantage une question de morale que de légitimité. Aucune loi n'interdit la chose mais, moralement parlant, il faudrait s'abstenir d'en faire des copies et il ne faudrait pas priver les . . .

Mme Nycum: Techniquement parlant, pour moi il s'agit d'une violation de la Loi sur le droit d'auteur, qui est une loi fédérale, chaque fois que quelqu'un fait une copie. Je ne pense pas que ces copies puissent être justifiées par la notion de juste utilisation, notion qui permettrait aux contrevenants d'échapper aux sanctions prévues. Toutefois, il y a rarement des poursuites intensives pour différentes raisons, ne serait-ce que le coût de l'appareil judiciaire, de sorte que tout le monde continue. C'est un problème, nous le savons, cela ne fait aucun doute. C'est une pratique qui est même considérée comme un problème grave.

M. Robinson (Etobicoke—Lakeshore): Vous avez dit que toutes les erreurs et tous les oublis qui entâchent l'utilisation des ordinateurs représentent probablement des pertes financières beaucoup plus considérables que tous les autres actes intentionnels. J'ai peine à le croire. Les gens sont-ils à ce point stupides et incapables d'utiliser les ordinateurs et les équipements informatiques qu'ils font à ce point des erreurs, qu'ils oublient tellement de choses que les coûts deviennent à ce point phénoménaux? Si c'est exact, ne pourrait-on pas conclure que cela devient un véritable poste budgétaire? Vous dites que vos budgets ne prévoient nullement la fraude mais je ne doute pas qu'ils prévoient les erreurs et les omissions.

Mme Nycum: En premier lieu, nous devons je crois accepter ceux qui critiquent les gens qui disent que le crime informatique n'est pas vraiment un problème et que toute proportion

[Text]

occasioned by human error it is less of a problem. I know myself that I make many more mistakes than I ever do an intentionally wrongful act, and I think that is probably fairly typical of human behaviour.

Whether errors and omissions are a cost of doing business—I am quite sure that they are so considered, and in fact one can buy insurance against them.

Mr. Robinson (Etobicoke—Lakeshore): Do you feel that there is a real problem in the United States with the lack of having a standard definition in most of the statutes with regard to computer crime; particularly since only 17 states have such legislation?

Mrs. Nycum: It depends on how broadly you would include the particular sections. You could get as high as 22, if you look at some of the financial sections which have to do with debit . . .

Mr. Robinson (Etobicoke—Lakeshore): But there are different definitions for the same terminology.

Mrs. Nycum: Yes, there are.

Mr. Robinson (Etobicoke—Lakeshore): Is any movement being made to standardize the definitions being used?

Mrs. Nycum: Not to my knowledge. I think each jurisdiction attempts to come up with what it feels is the best definition, both from the technical standpoint and from the standpoint of fitting in with its existing criminal law concept.

Mr. Robinson (Etobicoke—Lakeshore): Maybe it would be better if federal legislation were passed in this field that would standardize the definitions for all states involved. Would this be transgressing the state authorities?

Mrs. Nycum: I think the approach is to make it one of those things where there is shared jurisdiction; where both the federal and the state could have jurisdiction.

• 1705

As a practical matter, when the first Ribicoff bill was introduced it had a set of definitions, which for better or for worse were then copied by a number of the states which did indeed pass legislation. So there are some similarities in that respect.

Mr. Robinson (Etobicoke—Lakeshore): Mr. Beatty asked you something about the security of computers, and I see a statement here to the effect that computer manufacturers and service companies are providing more safeguards today to meet new and growing user demands for security. How costly is it to provide these safeguards, and how extensive are they? Is there any requirement, for instance, of the users to adopt and acknowledge security provisions?

[Translation]

gardée, par rapport aux pertes dues à l'erreur humaine, c'est un problème mineur. Je sais pertinemment bien que je fais personnellement davantage d'erreurs que je ne commets d'actes délictueux intentionnels, et j'imagine que c'est probablement une caractéristique de la nature humaine.

Cela dit, quant à ce demander si ces erreurs et ces omissions représentent un poste budgétaire pour les entreprises, je ne doute pas que ce soit effectivement le cas et d'ailleurs il est toujours possible de s'assurer contre les erreurs et les omissions de ce genre.

M. Robinson (Etobicoke—Lakeshore): Ne pensez-vous pas qu'il y ait actuellement aux États-Unis un problème très réel dû à l'absence de toute définition normalisée du crime informatique dans la plupart des lois, d'autant plus que 17 États seulement ont adopté des lois dans ce domaine?

Mme Nycum: Tout dépend de la portée des articles pertinents. On peut aller jusqu'à 22 infractions si l'on ajoute les articles à caractère financier relatifs au compte débiteur . . .

M. Robinson (Etobicoke—Lakeshore): D'accord, mais il n'empêche que la terminologie est la même, mais que les définitions sont différentes.

Mme Nycum: C'est exact.

M. Robinson (Etobicoke—Lakeshore): Y a-t-il une tendance à la normalisation des définitions utilisées?

Mme Nycum: Pas que je sache. Je pense que chaque secteur de juridiction s'efforce d'arriver à ce qu'il juge être la meilleure définition possible, tant du point de vue technique que du point de vue de son intégration à une notion existante en droit criminel.

M. Robinson (Etobicoke—Lakeshore): Il serait peut-être préférable d'avoir une législation fédérale qui garantirait automatiquement la normalisation des définitions pour tous les États. Cela reviendrait-il à transgresser les pouvoirs conférés aux États?

Mme Nycum: Je pense que l'on part du principe qu'il vaudrait peut-être mieux faire relever ce domaine des deux paliers de juridiction, le palier fédéral et celui des États.

Sous un angle pratique, lorsque le premier bill Ribicoff avait été déposé, il comportait toute une série de définitions qui pour le meilleur ou pour le pire ont été adoptées à leur tour par les États qui ont suivi. A cet égard, on relève donc certaines ressemblances.

M. Robinson (Etobicoke—Lakeshore): M. Beatty vous a posé quelques questions à propos de la protection des ordinateurs et je vois ici un texte selon lequel les fabricants d'ordinateurs et les entreprises de service offrent à l'heure actuelle davantage de garanties à cet égard en réponse justement au fait que les clients en exigent de plus en plus. Combien coûtent ces garanties et ces mesures de protection et quelle est leur portée? Ainsi, exige-t-on des utilisateurs qu'ils adoptent à leur tour des mesures de protection et qu'ils s'en servent?

[Texte]

Mrs. Nycum: By whom? Requirement by whom to . . .

Mr. Robinson (Etobicoke—Lakeshore): By the owners, operators, users, people who have access to the data.

Mrs. Nycum: But whose requirements would they be? The requirements established by the vendor to the user or . . . ?

Mr. Robinson (Etobicoke—Lakeshore): Well, the statement is made that the computer manufacturers and the service companies provide safeguards, but I suppose many of the users do not adopt the safeguards.

Mrs. Nycum: By contract, most of the vendors place the responsibility for the accuracy, timeliness and completeness of the service or the data on the user. They say: We have made every effort to put in what we think is a base of certain safeguards, but we are not going to represent and warrant anything to you along these lines; and it is your responsibility to use the device in the appropriate way or the service in the appropriate way.

Mr. Robinson (Etobicoke—Lakeshore): Do you have any specific recommendations that we might consider in our deliberations here? We are sort of in the embryo stage of developing some law on this whole question.

Mrs. Nycum: I congratulate you for addressing it so thoroughly. I think you have done a tremendous amount of homework, and I know the Department of Justice in particular has been spending a great deal of time and energy to come up with good legislation. You have done the right thing by looking at the experience of others to the extent they have had it.

I guess I have been concerned about the groups of wrongful acts that I discussed earlier and so would encourage you to include in your legislation sanctions against those types of wrongful acts that, as I said in this afternoon's presentation, seem to be occurring over and over again. I would recommend, for example, a provision directly concerning theft of services so that is clear because that is what is happening. To the extent that there might be any question in your minds as to the existence of good, sound legislation now, I would take care of that one.

I am concerned about communications, but I understand that in your code communications is effectively addressed so that is not a problem for you.

I have also been concerned, of course, with what happens with the information, particularly financial types of information, and that should be specifically addressed.

Mr. Robinson (Etobicoke—Lakeshore): From your paper I get the impression that you feel that there are certain safeguards—technical safeguards, I suppose—that should be used and carried out, but by the same token you feel that the way to deal with the matter is through criminal statutes. I am wondering whether you have considered whether there should in fact be this legislation that was not criminal in nature to

[Traduction]

Mme Nycum: Qui donc? Qui exigerait . . .

M. Robinson (Etobicoke—Lakeshore): Les propriétaires, les exploitants, les utilisateurs, tous ceux qui ont accès aux données.

Mme Nycum: Et qui établirait les critères? S'agirait-il de conditions imposées par le vendeur à l'utilisateur . . .

M. Robinson (Etobicoke—Lakeshore): Il est dit en fait que les fabricants d'ordinateurs et les entreprises de service offrent certaines garanties mais j'imagine qu'un certain nombre d'utilisateurs ne les adoptent pas.

Mme Nycum: La plupart des vendeurs précisent dans les contrats que tout ce qui concerne le service ou les données—précision, exactitude et intégralité—incombe à l'utilisateur. Les fabricants disent ceci: Nous avons fait tout ce que nous avons pu pour intégrer certaines mesures de sécurité que nous jugeons fondamentales, mais nous ne vous garantissons rien car c'est à vous à utiliser le matériel ou les services à bon escient.

M. Robinson (Etobicoke—Lakeshore): Auriez-vous des recommandations précises à nous formuler ici? Nous voulons élaborer une législation à cet égard mais nous n'en sommes encore qu'à nos premiers tâtonnements.

Mme Nycum: Je vous félicite d'avoir pris la peine d'approfondir le sujet à ce point. Vous avez fait je crois un travail préparatoire considérable et je sais notamment que le ministère de la Justice a consacré énormément de temps et d'efforts pour que la législation soit bonne. Vous avez fait ce qu'il fallait faire en commençant par étudier l'expérience des autres.

Vous vous êtes penché je crois sur les catégories d'agissements répréhensibles dont j'ai déjà parlé et je vous encouragerai donc à intégrer dans la législation les sanctions punissant ces catégories d'actes répréhensibles qui, comme je l'ai dit cet après-midi, semblent présenter un caractère répétitif. Je vous recommanderais ainsi une disposition touchant expressément le vol de services, une disposition expresse parce que c'est précisément cela qui se produit tous les jours.

Quant à moi, je ne m'inquiéterais pas du fait qu'à l'heure actuelle il n'y a peut-être aucune législation complètement satisfaisante à cet égard. Le problème des communications m'inquiète un peu, mais apparemment votre législation prévoit déjà le cas de sorte qu'il ne devrait pas s'agir d'un problème pour vous.

Je m'intéresserais également au problème de l'utilisation des données, et surtout des données à caractère financier.

M. Robinson (Etobicoke—Lakeshore): À la lecture de votre document, j'ai l'impression que selon vous il y aurait certaines mesures de protection—des solutions techniques j'imagine—qu'il faudrait utiliser mais d'autre part vous semblez dire que le problème devrait être réglé par le biais du Code criminel. Vous êtes-vous demandé si toute cette question de l'utilisation des ordinateurs et de l'accès au système informatique ne pourrait pas plutôt relever d'un code civil plutôt que criminel?

[Text]

control the whole question of the use of computers and access to computers.

Mrs. Nycum: Do you mean like seat belt legislation, the equivalent of a seat belt law or something like that?

Mr. Robinson (Etobicoke—Lakeshore): I suppose you could analogize it that way if you like. In other words, could you take civil legislation rather than criminal in nature, or should there be both?

• 1710

Mrs. Nycum: I see the future as bringing something to bear in the U.S. That is the only jurisdiction I am competent to even consider talking about. There will be a combination of legislation or simply court decisions which interprets ordinary standards of due care, so that safeguards will be imposed on people who are in the situation of either providing or using computer systems. The lack of some of these things will show an absence of due care and thus negligence and thus a duty which has been owed and breached to some group of foreseeable people, and liability will ensue. I find that is in my crystal ball of what will happen, at least in the U.S.

Mr. Robinson (Etobicoke—Lakeshore): Basically, as I understand it, the criminal law in the United States is within the jurisdiction of each individual state . . .

Mrs. Nycum: Yes.

Mr. Robinson (Etobicoke—Lakeshore): —whereas in Canada it is just the opposite. It would seem to me the only way the federal Government of the United States would be able to deal with the matter would be to legislate at a federal level with a piece of legislation of a civil nature that would be applicable to all states.

Mrs. Nycum: We have a proposed criminal piece of legislation which would be applicable to certain groups of computers and computer systems, which is very, very broad, as a matter of fact, when you really look at that definition.

Mr. Robinson (Etobicoke—Lakeshore): But if it is criminal in nature, then it would have to be accepted by all the states, would it not?

Mrs. Nycum: It would apply to those particular computer systems that are defined under the law. I do not have a copy of it right in front of me; but as I recall, it would apply to governmental ones, financial institutions, federal government installations, federally insured financial institutions and people providing services, I think. That can get to be a fairly broad . . .

Mr. Robinson (Etobicoke—Lakeshore): There is the whole question that employees, users of computers and people who have access, either legitimately or illegitimately, to a data bank should have a code of ethics or a code of conduct. I think in your notes you call it "codes of conduct". I suppose it is the same thing as a code of ethics. Has there been any development of this at all? Has it been enunciated in any way? Has it

[Translation]

Mme Nycum: Un peu sur le modèle de la législation relative aux ceintures de sécurité, c'est cela?

M. Robinson (Etobicoke—Lakeshore): Oui, j'imagine que cette analogie pourrait être valable. En d'autres termes, faudrait-il procéder par voie civile plutôt que criminelle ou faudrait-il les deux?

Mme Nycum: Je crois que les États-Unis nous apporteront quelque chose à l'avenir. C'est d'ailleurs le seul pays au sujet duquel je sois en mesure de parler avec quelque compétence. Ou bien il y aura une combinaison de mesures législatives, ou bien l'on s'en tiendra à des décisions judiciaires lorsqu'il s'agira d'interpréter les normes ordinaires de diligence afin que ceux qui se serviront des ordinateurs ou qui fourniront leurs services aux autres soient assujettis à certaines mesures de protection. Un manquement constituera un défaut de diligence, et partant une négligence, c'est-à-dire un manquement à une obligation envers un groupe précis. Celui qui se sera comporté ainsi sera donc tenu responsable. Enfin, à mon avis, c'est ainsi qu'évolueront les choses aux États-Unis.

M. Robinson (Etobicoke—Lakeshore): À ma connaissance, le droit pénal aux États-Unis relève de la compétence de chaque État . . .

Mme Nycum: Oui.

M. Robinson (Etobicoke—Lakeshore): . . . alors qu'au Canada c'est tout à fait le contraire. Il me semble donc que la seule façon dont le gouvernement fédéral des États-Unis puisse résoudre le problème, est de légiférer au niveau fédéral, d'adopter une loi civile applicable à tous les États.

Mme Nycum: Nous avons proposé un projet de loi pénale qui porterait sur certains groupes d'ordinateurs et de systèmes informatiques; il s'agit donc d'une définition très, très vaste.

M. Robinson (Etobicoke—Lakeshore): Toutefois, s'il s'agit d'un projet de loi pénale, alors il faudra que tous les États l'acceptent, n'est-ce pas?

Mme Nycum: Il porterait sur les systèmes informatiques définis par la loi. Je n'ai pas un exemplaire en main, mais si ma mémoire est bonne, le projet de loi s'appliquerait aux systèmes informatiques gouvernementaux, à ceux des institutions financières, des installations gouvernementales fédérales, des institutions financières assurées par le fédéral ainsi qu'aux personnes fournissant des services par l'entremise de ces systèmes. Or, cela est plutôt . . .

M. Robinson (Etobicoke—Lakeshore): Il y a aussi toute cette question de l'accès, soit légitime soit injustifié à une banque de données par des employés, des utilisateurs des ordinateurs et d'autres personnes, qui rendrait nécessaire l'existence d'un code de déontologie. Je crois que dans vos notes, vous vous servez de l'expression «code de conduite» à ce sujet. Cela correspond probablement à un code de déontologie.

[Texte]

been written down? Do you have a number of suggestions that would cover this whole area?

Mrs. Nycum: It is an interesting area, indeed. Several of our computer societies in the U.S. . . . in particular, the ATM is one—worked on a code of conduct, and we chose “conduct” because it was a term of what people would actually do. It would be the way they would conduct themselves. That has been adopted by the ATM, and there are several other organizations like the IEEE computer society which have them. They have not been tested, and it has been difficult to get a consensus of what is an unethical or an ethical act in a particular situation.

In Donn Parker's new book, I think he again refers to some of the studies that were done on that area and the experience which has been found to date.

The computer profession is changing and becoming an older, mature group of folk, but it is still has a number of people entering it who do not come from other established professions and who bring with them no intuitive feeling about what is right and wrong to do with computers.

Indeed, in the early days of the development, people shared all the time. They are continuing that feeling now with these mass-produced programs in that they learn from each other by sharing materials without regard to property concepts. A number of providers of computer programs now are putting them into the public domain intentionally, saying: Go use mine. So there is confusion, either deliberate or legitimate, as to one that has been placed in the public domain and one that has not, in the minds of people; at least, in the neighbourhoods around where I live in the bay area in San Francisco.

• 1715

Mr. Robinson (Etobicoke—Lakeshore): Could you tell me something about the difficulty in detecting computer crime? Is there sufficient sophisticated equipment to do this? Is it lacking? Are inroads being made to do this very thing? To what extent can we say there is sophistication in detection equipment so that people would be deterred from getting involved in computer crime, as we call it?

Mrs. Nycum: The detection has increased dramatically in sophistication. The detection is accomplished to some extent by tools, software tools, for example. There are programs that can look at other programs and data and see whether something has gone on that should not have gone on.

But it has largely been a case of educating the people who would use these tools. Those people will be auditors; internal and external auditors. They will be law enforcement personnel; that is, policemen and people who are concerned in prosecution. These folks have had thrust upon them within the last several years a technology which they were not trained in at all. It was not part of their job description to know about

[Traduction]

J'aimerais donc savoir si l'étude de cette question a été poussée. En a-t-on discuté ou a-t-on consigné des idées là-dessus? Avez-vous quelques propositions à ce sujet?

Mme Nycum: C'est certainement un domaine intéressant. D'ailleurs, bon nombre de sociétés informatiques américaines, comme l'ATM, ont travaillé à l'élaboration d'un tel code, et si nous avons choisi le terme «conduite», c'est parce que cela correspondait à ce que les gens font vraiment. J'entends par là que cela porte sur la façon dont les gens se conduiront. Ce code a donc été adopté par l'ATM et quelques autres organisations comme l'IEEE. Cela dit, étant donné que jusqu'à maintenant, aucune circonstance n'a nécessité le recours à ce code, il a été difficile d'obtenir une idée commune de ce qui est acceptable ou non sur le plan de la déontologie, dans une situation donnée.

Je crois que le nouveau livre de Don Parker mentionne certaines études effectuées dans ce domaine et les cas relevés à ce jour.

L'informatique est en train d'évoluer, et ceux qui oeuvrent dans ce domaine ont vieilli et ont mûri, mais il y a encore bon nombre de gens qui se joignent à cette profession sans avoir exercé d'autres professions au préalable, et qui n'ont donc aucune perception de ce qui est acceptable et inacceptable par rapport aux ordinateurs.

Lorsque la profession en était à ses débuts, les gens partageaient tout le temps. Ils continuent à être favorables à cela, maintenant qu'il existe des programmes produits en grande série, car ils apprennent les uns des autres en mettant leur travail en commun sans tenir compte des questions de propriété. D'ailleurs, certains fournisseurs de programmes informatisés les diffusent en public intentionnellement en enjoignant aux gens d'aller s'en servir. Il y a donc une confusion, soit légitime soit délibérément causée, lorsqu'il faut savoir ce qui est du domaine public et ce qui ne l'est pas. C'est tout au moins la situation dans les quartiers de San Francisco où j'habite, c'est-à-dire dans la région longeant la baie.

M. Robinson (Etobicoke-Lakeshore): Pouvez-vous me dire quelque chose au sujet des difficultés qu'il y a à déceler les infractions relatives aux ordinateurs? Dispose-t-on de moyens techniques assez évolués pour le faire? Au contraire, en manquons-nous? Fait-on des progrès à cet égard? Dans quelle mesure les moyens actuels dissuadent-ils de commettre ces infractions?

Mme Nycum: Les moyens de détection sont beaucoup plus poussés qu'avant. On réussit à déceler les infractions grâce, entre autres, à des mécanismes de logiciel. Il s'agit donc de programmes vérifiant d'autres programmes et données afin de voir si quelque chose d'anormal s'est passé.

Toutefois, il a fallu enseigner l'utilisation de ces programmes à des vérificateurs, à la fois internes et de l'extérieur. Il faudra aussi instruire les policiers et ceux qui travaillent dans un domaine connexe à la poursuite de la même chose. Ces dernières années, tous ces gens ont été obligés de traiter de questions relatives à une technologie sur laquelle ils n'ont reçu aucune formation. La connaissance des ordinateurs ne faisait

[Text]

computers, and suddenly they have found it necessary. We have been quite impressed with the way the organizations have risen to that challenge. There is now a subset of the computer field called computer security people, who are worried about implementing precautions in the beginning; and then there are the computer auditors, who are interested in finding out whether controls are in place, designing controls and checking to see that the controls are being followed; and then the law enforcement people, who are increasingly knowledgeable in tracking a computer crime and then prosecuting it.

Mr. Robinson (Etobicoke—Lakeshore): You made mention of the penalties earlier on, and you indicated that they were quite substantial. I note from the California penal code that the maximum is \$5,000 and up to 16 months in prison. Do you feel that is big enough, if you let the punishment fit the crime? People may be bilking an institution out of, as you suggested, billions of dollars . . .

Mrs. Nycum: Yes, it can depend on what that crime has actually been. I know that in the original Ribicoff bills it was, boom, a \$50,000 fine; and people were saying: What, for making an unauthorized Snoopy calendar? The other end of the coin is that the sentences that had been meted out in the past for even very, very large thefts had been two months—something of that sort—typically based on the fact that this was a first-time criminal and no damage had been done to lives or property in the traditional sense.

So there was a hue and cry on both sides; one hue and cry saying they are stealing all this money and they are only going to get charged this for it, and the other side saying: What, you are hitting me for making an unauthorized Snoopy calendar with this huge fine?

So I think the balance is being struck at some multiple—and I think that is Mr. Nelson's approach—some multiple of the amount of the loss as the fine.

Mr. Robinson (Etobicoke—Lakeshore): I do not see that provision in the California penal code, but maybe the case you are referring to was not tried in California.

Mrs. Nycum: The California people really want . . . There was a lot of testimony at the hearings that there ought not to be any law at all addressed to this, by the computer professionals, who were saying: Do not make us pay \$50,000. So it was deliberately lowered to a number that was more in line with other fines and imprisonment standards in the penal code.

Mr. Robinson (Etobicoke—Lakeshore): You indicated also previously in your remarks that Sweden, Norway, the United Kingdom, and Germany, among others, had passed laws on computer crime. Are they extensive in nature? Do you know much about them?

[Translation]

pas partie des exigences de leurs fonctions, et tout d'un coup, elle est devenu nécessaire. Cela dit, nous avons été très impressionnés par la façon dont les organismes font face à la situation. Il existe maintenant une branche connexe au domaine de l'informatique, celle des services de sécurité en informatique, dont les membres s'occupent des précautions à prendre dès le départ. Il y a ensuite les vérificateurs d'informatique, qui cherchent à voir quelles mesures de contrôle sont en place et qui vérifient si on s'y conforme. En dernier lieu viennent les services policiers, qui savent de plus en plus comment déceler une infraction commise par ordinateur et intenter les poursuites appropriées.

M. Robinson (Etobicoke—Lakeshore): Vous avez mentionné les sanctions; vous avez dit qu'elles sont très sévères. À cet égard, j'ai remarqué dans le Code pénal de Californie qu'on peut imposer une amende maximale de \$5,000 et jusqu'à 16 mois de prison. Croyez-vous que cela suffise, compte tenu du fait que les peines doivent correspondre à la gravité du crime? Dans certains cas, certaines personnes pourraient avoir soutiré des milliards de dollars d'un établissement . . .

Mme Nycum: Oui, cela peut dépendre de la gravité du crime. Je sais que les projets de loi Ribicoff proposaient d'abord une amende de \$50,000; or, les gens se disaient: Une amende aussi lourde pour une bagatelle comme dessiner un calendrier à l'effigie de Snoopy? Par contre, les sanctions imposées par le passé, même dans le cas de vols considérables étaient de deux mois de prison, ou quelque chose du genre, parce qu'il s'agissait d'une première infraction et parce qu'aucune atteinte n'avait été portée ni à la vie ni à la propriété dans le sens traditionnel de ces termes.

On a donc assisté à une levée de boucliers des deux côtés. D'une part, on disait qu'il y avait eu des vols d'argent considérables et que les coupables n'allaient écoper que de peines très légères alors que, d'autre part, on demandait pourquoi on imposait des amendes aussi élevées pour des vétilles comme dessiner un calendrier non autorisé à l'effigie de Snoopy.

A mon avis donc, et à celui de M. Nelson aussi, je crois, une somme correspondante à un multiple du montant volé constituerait une amende juste.

M. Robinson (Etobicoke—Lakeshore): Je n'ai pas vu de telles dispositions dans le Code pénal de la Californie, mais peut-être vous reportez-vous à une affaire qui n'a pas été jugée dans cet état.

Mme Nycum: Ce que les Californiens veulent vraiment . . . Lors des audiences, les spécialistes en informatique ont fait valoir qu'il ne devrait pas y avoir de loi portant précisément là-dessus; ils ne voulaient pas payer des amendes de \$50,000. On a donc réduit le montant des amendes envisagées afin qu'il soit davantage comparable aux amendes et autres peines prévues dans le Code pénal.

M. Robinson (Etobicoke—Lakeshore): Plus tôt, vous avez également remarqué que la Suède, la Norvège, le Royaume-Uni et l'Allemagne, entre autres, ont adopté des lois relatives aux infractions relatives aux ordinateurs. Êtes-vous au courant de leur contenu? Ont-elles une portée très vaste?

[Texte]

• 1720

Mrs. Nycum: No, they are not extensive in nature. I do not know very much about them yet, and my information comes essentially from the gentleman who is chief of police in Oslo and who has published a report on international computer crime. That report is available; unfortunately, I do not have it here with me, but I could make it available. This report indicates that most of these laws are really rather piecemeal and certainly not at all comprehensive, but they are an indication of a direction of concern and just a trend.

Mr. Robinson (Etobicoke—Lakeshore): Could you send us a copy of that report, since it is available?

Mrs. Nycum: I would be delighted to.

Mr. Robinson (Etobicoke—Lakeshore): Would it be fair to say that the United States is really in the forefront of the computer law business at the present time?

Mrs. Nycum: In the nature of computer crime legislation?

Mr. Robinson (Etobicoke—Lakeshore): Yes.

Mrs. Nycum: I think we are probably so regarded. In fairness to our friends in Sweden, I believe they are also very active in this respect.

Mr. Robinson (Etobicoke—Lakeshore): What do you suggest for correction with regard to the question of detection? What corrective measures could be taken that are not being taken now?

Mrs. Nycum: I know that the RCMP has been involved in this area for some years, and in a very sophisticated way. My suggestions would be to really focus on education, both for the victim to detect that something has happened to himself, where it may, and to educate the public authorities in detection mechanisms in the situation in which a possible act has been reported.

We have had some experiences in the United States in which victims have reported that having determined by themselves, on their own account, that there has been a perpetration they have then confronted the perpetrator and terminated the perpetrator only to find that the prosecution was declined by the public authorities. Then the alleged perpetrator would turn around and sue the alleged victim for wrongful discharge, disparagement or something of this sort. This then was a deterrent, not to perpetration, but to reporting of acts of perpetration.

Mr. Robinson (Etobicoke—Lakeshore): My last question. In your view, is there a degree of urgency with regard to passing legislation in this field, whether it be civil legislation or amendments to the Criminal Code?

Mrs. Nycum: My answer to the urgency depends on what exists, how complete the existing laws are with respect to catching events of wrong-doing or criminal acts involving computers.

In the event that there are needs—in other words, that you cannot prosecute someone for an obvious wrongful act because

[Traduction]

Mme Nycum: Non, elles ne sont pas de très vaste portée. Je n'en sais pas encore beaucoup à leur sujet, et mes renseignements proviennent surtout du chef de police d'Oslo, qui a publié un rapport sur les crimes relatifs aux ordinateurs à l'échelle internationale. Ce document est disponible mais malheureusement, je n'en n'ai pas d'exemplaire en main. Je peux toutefois l'obtenir. Il indique que la plupart des lois sont plutôt partielles, enfin certainement pas globales, mais elles illustrent une tendance et certaines préoccupations.

M. Robinson (Etobicoke—Lakeshore): Pouvez-vous nous envoyer un exemplaire de ce rapport étant donné qu'il est disponible?

Mme Nycum: Très volontiers.

M. Robinson (Etobicoke—Lakeshore): Est-il exact de dire que les États-Unis sont le fer de lance du mouvement de législation en matière d'infractions commises par ordinateurs?

Mme Nycum: Vous parlez de l'adoption de lois relatives aux crimes relatifs aux ordinateurs?

M. Robinson (Etobicoke—Lakeshore): Oui.

Mme Nycum: Je crois qu'on nous considère comme cela. Toutefois, en toute justice à l'endroit de nos amis suédois, je crois qu'ils sont également très actifs à cet égard.

M. Robinson (Etobicoke—Lakeshore): Quelle mesure corrective proposez-vous de prendre pour qu'on décèle mieux ces infractions?

Mme Nycum: Je n'ignore pas que la GRC travaille là-dessus depuis déjà quelques années, et d'une façon très poussée. Cela dit, je proposerais qu'on enseigne à la victime les moyens de déceler que quelque chose d'anormal s'est produit, le cas échéant, et de montrer aussi aux autorités publiques les mécanismes de détection qu'il faut utiliser lorsqu'on rapporte un incident.

Aux États-Unis, dans certains cas où les victimes s'étaient rendu compte qu'on avait commis un abus quelconque dans ce domaine, on a confronté le coupable et mis fin à ses activités pour se rendre compte que les autorités publiques refusaient de poursuivre l'inculpé. Ensuite, ce dernier a poursuivi la victime présumée pour renvoi injustifié, atteinte à la réputation ou quelque chose de semblable. Ces circonstances n'ont donc pas servi à dissuader de perpétrer de tels actes mais bien de les déclarer.

M. Robinson (Etobicoke—Lakeshore): J'en suis à ma dernière question. À votre avis, est-il urgent d'adopter une législation dans ce domaine, qu'il s'agisse de lois relevant du civil ou d'amendements au Code pénal?

Mme Nycum: Pour répondre, je dois savoir dans quelle mesure les lois actuelles permettent de déceler les infractions relatives aux ordinateurs.

Si toutefois il y a des carences à cet égard, autrement dit s'il est impossible de poursuivre quiconque ayant manifestement

[Text]

it is not technically a crime—I would say there is a tremendous urgency because this is the type of thing which is now a way of life with increasing use of computers and with, as I said earlier, the democratization of that use. That would my answer. In the U.S., in some states it was absolutely essential to move very briskly. In other states it was not so necessary because of the underlying . . .

Mr. Robinson (Etobicoke—Lakeshore): When you use the term “democratization” of computer crime, it seems to me a bit oxymoron.

Mrs. Nycum: It is not my term. It should have quotes around it because it belongs to a well-known computer security consultant who has used it, and it seems to have caught on.

Mr. Robinson (Etobicoke—Lakeshore): Thank you very much.

Mrs. Nycum: Thank you.

The Chairman: Maybe I will ask this out of curiosity. If you used one of these laws in the United States, as far as California is concerned, I mean, which side were you defending? Was it someone who has been charged? Or were you on the safe side?

• 1725

Mrs. Nycum: Well, I typically am involved as counsel to a victim who is saying: What can we do? So it is from the victim's standpoint that I look at these things. When the question was asked about the person who has had his programs stolen, I felt very close to that victim because that has indeed happened to some of my clients.

I have been asked sometimes to advise on the technical aspects to the prosecutors and occasionally to defence lawyers who are trying to learn how to defend accused people.

The Chairman: So if there was a civil case where a person had to recover some moneys, you could act on behalf of the victim. But for the criminal part of it, you would . . .

Mrs. Nycum: Yes. I do not personally practice criminal law, but many of these situations have a civil aspect as well, particularly in the taking of software.

The Chairman: With all the legislation you are aware of, would you say that California and Florida are the most comprehensive probably of those who are tackling the issue? Perhaps it was because they needed a net in those states more than in others; I do not know. It seems that they are more comprehensive and cover a lot of aspects.

Mrs. Nycum: Yes. Another jurisdiction I find to have a well-thought-out law is Illinois. It is curious that the first states were able to do a comprehensive job, but some of the later ones I do not regard as being quite as good models.

[Translation]

perpétré une infraction simplement parce que ce genre d'abus n'est pas considéré comme un crime sur le plan technique, alors c'est très urgent, car ce genre de chose devient de plus en plus courant étant donné la généralisation des ordinateurs et, comme je l'ai mentionné plus tôt, la démocratisation de leur usage. Voilà pour ma réponse. Aux États-Unis, dans certains États, il a été impératif d'agir très rapidement alors que dans d'autres, cela n'était pas aussi pressant à cause de . . .

M. Robinson (Etobicoke—Lakeshore): Lorsque vous parlez de «démocratisation», cela me semble une image contradictoire, un oxymoron.

Mme Nycum: Le terme n'est pas de moi. Il devrait d'ailleurs être mis entre guillemets parce qu'il a d'abord été utilisé par un consultant en sécurité des ordinateurs; il semble s'être répandu.

M. Robinson (Etobicoke—Lakeshore): Merci beaucoup.

Mme Nycum: Merci.

Le président: Je vais poser la question suivante par curiosité peut-être. Lorsque vous avez eu recours à l'une de ces lois aux États-Unis, plus précisément en Californie, de quel côté étiez-vous, c'est-à-dire qui défendiez-vous? Un accusé ou une victime, ce qui est plus facile?

Mme Nycum: Et bien, d'habitude je suis au service d'une victime qui se demande ce qu'elle peut faire. Je vois donc ces choses du point de vue d'une victime. En conséquence, quand on m'a interrogé au sujet de la personne dont on a volé les programmes, j'ai ressenti une grande sympathie pour elle parce que certains de mes clients ont précisément été victimes de cela.

Parfois, des procureurs m'ont demandé des conseils techniques ainsi que des avocats de la défense qui s'instruisaient sur la façon de défendre des accusés dans de telles circonstances.

Le président: Donc, si une personne essayait de récupérer de l'argent grâce à une action intentée au civil, vous pourriez la représenter. Toutefois, pour ce qui relève du droit pénal, vous . . .

Mme Nycum: Oui. Je n'exerce pas au pénal, mais bon nombre de ces situations relèvent aussi du droit civil, particulièrement dans les cas où il y a vol de logiciel.

Le président: Compte tenu de toutes les lois que vous connaissez, d'après vous, celles de la Californie et de la Floride vous paraissent-elles avoir la plus vaste portée? Peut-être est-ce ainsi parce qu'on avait davantage besoin de se protéger dans ces États que dans d'autres; je l'ignore. Enfin, il me semble qu'elles sont effectivement plus vastes, qu'elles couvrent davantage de choses.

Mme Nycum: Oui. De plus, l'Illinois semble aussi avoir adopté une loi soigneusement élaborée. Il est assez curieux de remarquer que les premiers États à se pencher sur ce dossier ont réussi à fournir un projet global alors que certains des derniers venus ne me paraissent pas avoir produit d'aussi bons modèles.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): Madam Chairman, I noted that our witness today, Mrs. Nycum, spoke extensively in relation to, and in part, from . . . I asked questions on this document before us, which was testimony given by her and Mr. Parker before the United States House of Representatives. I wonder if this could be appended to our minutes for today. It is in both official languages.

The Chairman: Thank you, Mr. Robinson. Yes. Agreed. Thank you, Mrs. Nycum, for appearing before us today and for the clarification you gave to us. We will certainly try to make good use of your information so as to come up with some solutions the Canadian way.

Mrs. Nycum: I applaud you for your activities. I am very very honoured to be here today. Thank you.

The Chairman: Thank you. The meeting is adjourned.

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Madame le président, j'ai remarqué que notre témoin d'aujourd'hui, M^{me} Nycum, s'est souvent reportée à un document dans ses interventions . . . J'ai déjà posé des questions sur le document que nous avons en main, et qui est constitué par le témoignage qu'elle et M. Carter ont présenté devant la Chambre des représentants du Congrès américain. J'aimerais donc savoir si on peut l'annexer à notre procès-verbal d'aujourd'hui. Il a été fourni dans les deux langues officielles.

Le président: Merci, monsieur Robinson. Oui, d'accord. Merci, madame Nycum, d'avoir bien voulu comparaître devant nous aujourd'hui et de nous avoir apporté vos éclaircissements. Nous nous efforcerons certainement de mettre à profit les renseignements que vous nous avez communiqués, dans notre recherche d'une solution canadienne.

Mme Nycum: J'applaudis votre entreprise et ce fut un grand honneur pour moi d'être ici aujourd'hui. Merci.

Le président: Merci. La séance est levée.

APPENDIX "COMP-3"

TESTIMONY BY DONN B. PARKER AND SUSAN HUBBELL NYCUM
ON COMPUTER CRIME

Before the U.S. House of Representatives Subcommittee of the
Judiciary Committee on Constitutional and Civil Rights
September 23, 1982, Washington, D.C.

IntroductionDonn. B. Parker

My name is Donn B. Parker. I have extensive qualifications in the computer field, having worked for 30 years in computer programming and computer systems management. For the past 13 years of my career, I have been a researcher and consultant specializing in the computer crime problem and computer security. I have a Master of Arts degree in mathematics from the University of California at Berkeley. I am currently a senior management systems consultant in the Information Systems Management Department at SRI International, Menlo Park, California. The statements included herein are my own and do not necessarily represent those of SRI International or any clients of SRI.

I have published widely. I wrote the definitive book on computer crime, Crime by Computer, in 1976; a new book, Fighting Computer Crime, will be published in January 1983. In addition, I have written two books for the professional audience, Computer Security Management and Ethical Conflicts in Computer Science and Technology. My SRI associates, Ms. Susan Hycum, and I produced the definitive manual on computer crime investigation and prosecution, Criminal Justice Resource Manual on Computer Crime, for the Bureau of Justice Statistics of the U.S. Department of Justice.

Susan Hubbell Nycum

My name is Susan Hubbell Nycum. I have practiced computer law for nearly 20 years and have been involved in the legal aspects of computer abuse for 13 years. I am a partner in the national law firm of Gaston, Snow and Ely Partlett and am resident in the firm's Palo Alto, California, office. I am the partner in charge of the firm's Computer and High Technology Group.

I wrote the first articles on the legal aspects of computer crime, which appeared in the American Bar Association Journal, the Rutger's Journal of Computers and the Law, the University of Pittsburgh Law Journal, and others. I have performed studies of the legal aspects of

computer abuse for the National Science Foundation, the Bureau of Justice Statistics in the Department of Justice, and the Office of Technology Assessment, as well as for private organizations.

I am a past chairman of the American Bar Association Section of Science and Technology, a director of the Computer Law Association, one of three American Bar Association members of the National Conference of Lawyers and Scientists. I have represented the United States as one of a three person State Department led delegation to the OECD meeting on national vulnerabilities, which focused heavily on computer crime.

The Changing Nature of Business and White-Collar Crime

As we enter the information age, business and white-collar crime is changing significantly. Valuable assets are increasingly represented by information, an intangible property, and its processing, transmission, and storage are rapidly becoming the targets of crime. Such crime includes fraud, theft, embezzlement, larceny, sabotage, espionage, extortion, and conspiracy. Because of increasing automation throughout society, however, the following changes are occurring:

- New, greater requirements for trustworthy employees -- Data processing employees are entrusted with their employer's information assets with little likelihood of wrongdoing being discovered.
- New environment for business and white-collar crime -- Some automated information crimes occurring inside computers are invisible to victims. Moreover, the same computers compromised in the crimes are sometimes needed to obtain evidence of loss before it can be electronically erased.
- New forms of assets subject to criminal attacks -- Money as well as inventory, marketing, and other data in electronic forms that are stored in computers and on computer media such as magnetic tapes make computers the new business vaults containing the targets of crime.
- New criminal methods -- The technical methods used in most reported computer crimes are impersonating another computer user and data diddling (false data entry). These criminal methods are far safer for perpetrators than the relatively infrequently reported exotic and complex methods of programmed fraud such as Trojan horse attacks (inserting secret instructions in legitimate computer programs), superzapping (unauthorized use of utility programs), or wiretapping.

- New time scale -- While business crime has traditionally been measured in minutes, hours, days, and weeks, we now measure some automated crimes in the computer time scale of a few thousandths and millionths of seconds.
- New, wider geographical scale -- The geography of business crime has broadened. A fraud in a computer connected to the dial-up telephone system in Washington, D.C. could be committed from a terminal in a telephone booth in Japan or anyplace else in the world.

The Nature of Computer Crime

For purposes of study of computer crime for criminal justice, computer crime is defined as any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution. Computer crime is not a single type of crime different from other crimes. Rather, nearly all kinds of crimes can be committed through computers or be computer mediated. In fact, we have documentation of crimes of every known type involving computers except a few violent crimes such as rape and aggravated assault.

People can use computers in only four ways to perpetrate crimes:

- A computer can be the object of attack. For example, international terrorists have used bombs and submachine guns to attack at least 28 computer centers of multinational companies and government agencies in Italy and France over the past 4 years.
- A computer can be the subject of a crime by providing the automated mechanisms to modify and manipulate new forms of assets such as computer programs and information representing money.
- A person can use a computer as a tool or instrument for conducting or planning a crime. A stockbroker used a computer to produce forged investment statements showing huge profits to deceive his clients and steal \$53 million.
- A person could use only the symbol of the computer to intimidate or deceive. The same stockbroker told his clients that he was able to make such huge profits on rapid stock option trading by using a secret computer program in a giant computer in a Wall Street brokerage. He had no such program nor access to the computer, but hundreds of clients were convinced enough to invest a minimum of \$100,000 each.

Computer criminals have tended to be young, highly motivated, trusted employees without previous criminal records. Thus, specific computer crime statutes are likely to have greater deterrent value for these individuals who see themselves as problem solvers, not as crooks, than for career criminals, especially by confronting the amateur criminals with the criminality of their acts. They are convinced that they do not hurt people or even organizations, just computers. More career criminals are engaging in computer crime, however, as they find their typical environments for crime being filled with computers.

As computer technology advances, a new kind of computer criminal, the system hacker, has emerged as an outgrowth of the phone phreaks of the 1960s. A serious epidemic of system hacking and computer program piracy is evident across the country as high school and college students learn computer methods and gain access to telephone terminals and personal microcomputers. Sometimes they even are encouraged by their instructors to engage in technological trespassing, electronic vandalism, and violation of proprietary rights to computer programs through copying. One computer program manufacturer estimates that two out of three of the copies of their products in use have not been paid for, although their profits are still so large that they do not worry about it very much. We hope to start a major study of these growing problems very soon to estimate their size and develop solutions. We believe that specific criminal statutes will act as an important deterrent and help solve these problems.

No valid statistics on the extent of computer crime committed or the losses exist. The many numbers quoted in the news media are not truly representative of experience because acceptable mechanisms for collecting comprehensive or valid statistical samples have not been established. A lack of concurrence for a definition of computer crime precludes comprehensive statistical evaluation. SRI has the largest collection of documentation of reported cases according to our definition; yet the tabulations of more than 1,000 cases of computer abuse that have occurred since 1958 worldwide represent only a few of all suspected cases.

More money is probably lost from all errors and omissions in the use of computers than is likely lost in all intentional acts. Nevertheless, we can and have controlled errors, and their cost is budgeted as a part of data processing. We do not predict or budget for fraud; its perpetration comes as an unpleasant surprise. Moreover, the size of individual, large-loss crimes has surpassed the accidental loss experienced by particular victims.

Computer crime has been identified as being easy to perpetrate. This notion is greatly oversimplified and incomplete. Some computer crimes have been relatively easy and safe to perpetrate, but only by those few people with sufficient skills, knowledge, resources, and access to assets. They would have been very difficult for anyone else. Certain small computer crimes have been rather simple to perform by

clerical employees with limited technical capabilities and minimal difficulty of access to assets; other crimes have been very complex. Automated crime is relatively insensitive to size of loss. Once a criminal act has been planned, taking \$100,000 or increasing it to \$1,000,000 is sometimes only a matter of adding three zeros.

All prosecutors I have questioned indicate that they have been, or would successfully be, able to prosecute all known computer crimes using existing criminal statutes. However, many of them also indicate difficulty in applying those statutes for purposes never anticipated when they were created, and few prosecutors understand the possibilities for new crimes not covered by existing statutes. The conviction rate of those indicted is very high based on limited known experience. Without specific computer crime statutes, it is easier for victims not to report their loss to avoid embarrassment or unwanted attention and prosecutors to avoid prosecuting the crime from a lack of knowledge about computers.

The Future of Computer Crime

On the basis of case-by-case studies working with victims and investigators, interviews with more than 30 perpetrators, and computer security reviews for clients, we make the following projections:

- The incidence of computer crime will increase because of the increasing number of computers and the automation of business activities.
- The use of computers for criminal purposes in bookmaking, drug distribution and sales, scams, and prostitution will grow beyond the few known cases. Electronic funds transfer systems offer attractive opportunities for fraud and rapid laundering of money as \$400 billion per day domestically and \$600 billion per day internationally are exchanged among interconnected bank computers and automated teller machines. Increasing use of data communications, voice data entry and computer output, optical data storage, video systems, and robots will also attract new forms of criminal activity. This requires that criminal statutes be comprehensive and technology-independent to avoid further rapid obsolescence of the law.
- The size of losses in significant cases will increase dramatically because of the concentration of information assets in computer and communications systems in fragile forms subject to powerful manipulation by computers. Consider the \$200 million Equity Funding Insurance fraud, the \$21 million bank embezzlement in Los Angeles, the \$10 million funds transfer fraud also in Los Angeles, the \$53 million securities fraud in Florida, the \$50 million commodity futures fraud in Denver, and the \$18 million inventory fraud in Chicago, which were all record-breaking cases of their types. Some analysts have meaninglessly disputed whether these cases are in fact computer crimes on the basis of several different definitions in use.

Each of 17 states with a computer crime statute has a different legal definition and, of course, no Federal legislation has yet been promulgated to settle this issue. Clearly, however, the use of computers in these cases contributed to creating the special environments, tools, and access to large amounts of financial assets with limited prevention and detection controls in place.

- The potential for increased protection of automated business activities is far greater than was ever possible in previous manually performed activities. That potential is now starting to be realized in modern computers. Computer manufacturers and service companies are providing more safeguards today to meet new and growing user demands for security. Although significant cases of business and white-collar crime will decrease, the increasing difficulty and danger of engaging in crimes involving computers will significantly increase the losses per case. We refer to this anticipated condition as the escalation of business crime.
- The escalation of business crime may create new vulnerabilities, even though a recent study by an American Federation of Information Processing Societies Task Group concluded that the resiliency of society and limited dependence on computers precludes major problems today. We believe that by using such technical safeguards as cryptography, advanced management controls, and codes of conduct stimulated in part by strong criminal statutes we can continue to limit risks inherent in the use of computer technology to an acceptable level.

Recommendations

In conclusion, we recommend careful legislative action to advance federal criminal laws to deter and prosecute crime in the information age. such legislation should focus on protection of information as a valuable asset subject to criminal acts by people with new technical capabilities and not just focus on rapidly changing computer technology. However, before enactment, all of the implications and effects of information age crime and proposed legislation should be identified and thoroughly reviewed in public by a national commission of inquiry to assure adequate attention from and support of the stakeholders.

(TRADUCTION)

APPENDICE "COMP-3"

TÉMOIGNAGE DE DONN B. PARKER ET SUSAN HUBBELL NYCUM
SUR LA CRIMINALITÉ INFORMATIQUE

Témoignage donné devant le Subcommittee on the Judiciary Committee on Constitutional and Civil Rights de la Chambre des représentants des États-Unis, le 23 septembre 1982, à Washington (D.C.)

IntroductionDonn B. Parker

Mon nom est Donn B. Parker. J'ai une longue expérience de l'informatique car j'ai travaillé 30 ans dans les domaines de la programmation et de la gestion des systèmes informatiques. Depuis treize ans, je fais de la recherche et j'agis à titre d'expert-conseil spécialisé dans le domaine de la criminalité et de la sécurité informatiques. Je possède une maîtrise en mathématiques de l'Université de la Californie à Berkeley. Je suis actuellement expert-conseil principal en matière de systèmes de gestion au Service de gestion des systèmes informatiques du SRI International à Menlo Park en Californie. Les opinions énoncées dans le présent document sont les miennes et ne représentent pas nécessairement celles de SRI International ou des clients de SRI.

J'ai publié de nombreux documents. J'ai écrit le livre le plus complet sur la criminalité informatique, Crime by Computer, publié en 1976; un livre intitulé Fighting Computer Crime paraîtra en janvier 1983. En outre, j'ai écrit deux livres à l'intention des spécialistes, Computer Security Management et Ethical Conflicts in Computer Science and Technology. Mes collègues du SRI, Mme Susan Nycum et moi-même avons produit le manuel faisant autorité sur les enquêtes et les poursuites judiciaires relatives à la criminalité informatique pour le Bureau of Justice Statistics du ministère de la Justice des États-Unis; il s'intitule Criminal Justice Resource Manual on Computer Crime.

Susan Hubbell Nycum

Mon nom est Susan Hubbell Nycum. Je pratique le droit de l'informatique depuis presque 20 ans et je traite des aspects juridiques des délits relatifs à l'informatique depuis près de 13 ans. Je suis associée dans le cabinet juridique de Palo Alto en Californie. Je suis chargée du Groupe de l'informatique et des techniques de pointe.

J'ai écrit les premiers articles sur les aspects juridiques de l'informatique qui ont paru dans le American Bar Association Journal, le Rutger's Journal of Computers and the Law, le University of Pittsburgh Law Journal et d'autres revues spécialisées. J'ai fait des travaux sur les aspects juridiques de la criminalité informatique pour la National Science Foundation, le Bureau of Justice Statistics du ministère de la justice, et le Office of Technology Assessment, ainsi que pour des organismes privés.

J'ai été président de la Section of Science and Technology de l'American Bar Association; je suis administrateur de la Computer Law Association, et l'un des trois membres de l'American Bar Association appartenant à la National Conference of Lawyers and Scientists. J'ai représenté les États-Unis au sein d'une délégation de trois personnes dirigée par le département d'État à la réunion de l'OCDE sur la vulnérabilité de la société informatisée qui a porté surtout sur la criminalité informatique.

L'évolution de la criminalité en col blanc

Depuis l'avènement de l'ère de l'information, la criminalité en col blanc subit de profondes transformations. L'information, un bien intangible, représente de plus en plus un avoir de grande valeur, et son traitement, sa transmission et son stockage deviennent rapidement les cibles de divers actes criminels: fraude, vol, détournement de fonds, sabotage, espionnage, extorsion et conspiration. Cependant l'automatisation croissante dans l'ensemble de la société entraîne les changements suivants:

- On a de plus en plus besoin d'employés fiables -- les employés chargés du traitement des données ont accès aux avoirs de leur employeur sous forme d'information, et les malversations risquent peut d'être découvertes.

- A la criminalité en col blanc correspond un cadre nouveau -- certains délits informatiques commis de l'intérieur des ordinateurs sont invisibles pour les victimes. De plus, il faut parfois utiliser les ordinateurs mêmes qui ont servi au délit pour prouver les pertes avant que les indices n'aient pu être effacés électroniquement.
- De nouvelles formes d'avoirs sont la cible des attaques des délinquants -- l'argent, ainsi que les données sur les stocks, sur les produits mis en marché et d'autres informations qui sont stockées sur ordinateur et sur des supports informatiques comme des bandes magnétiques font des ordinateurs des coffres-forts d'un nouveau genre.
- De nouvelles méthodes criminelles apparaissent -- les techniques utilisées dans la plupart des délits informatiques signalés consistent à se faire passer pour un autre utilisateur de l'ordinateur et à entrer de fausses données. Ces méthodes sont beaucoup plus moins risquées pour leurs auteurs que certaines techniques de fraude subtiles et complexes relativement moins fréquentes comme le "cheval de Troie" (l'addition d'instructions secrètes à des programmes informatiques légitimes), l'utilisation non autorisées de programmes utilitaires, ou l'écoute des lignes téléphoniques.
- Nouvelle échelle temps -- jusqu'à présent, les délits des cols blancs ont toujours été mesurés en minutes, en heures, en jours et en semaines; mais maintenant certains délits informatiques se mesurent à l'échelle du temps-machine c'est-à-dire en millièmes et millionièmes de seconde.
- Nouvelle échelle géographique plus vaste -- La géographie de la criminalité en col blanc s'est élargie. Une fraude touchant un ordinateur relié au réseau téléphonique commuté de Washington (D.C.) peut être commise au moyen d'un terminal installé dans une boîte téléphonique au Japon ou n'importe où dans le monde.

La nature de la criminalité informatique

Pour l'étude de cette notion du point de vue de la justice pénale, on définit la criminalité informatique comme tout acte illégal nécessitant une connaissance spéciale de l'informatique sur sa perpétration pour l'enquête sur le délit et pour les poursuites devant les tribunaux. Le délit informatique n'est pas un genre de délit unique, différent des autres, car presque tous les genres de délit peuvent être commis au moyen d'ordinateurs. En fait, il existe des rapports montrant que des actes criminels de tous les genres connus ont été commis au moyen de l'informatique, sauf quelques crimes avec violence comme le viol et les voies de fait.

On ne peut utiliser l'ordinateur que de quatre façons pour perpétrer un acte criminel:

- L'ordinateur peut être l'objet d'une attaque. Par exemple, ces quatre dernières années, des terroristes internationaux ont attaqué à la bombe et à la mitrailleuse au moins 28 centres informatiques de sociétés multinationales et d'organismes gouvernementaux en Italie et en France.
- L'ordinateur peut être l'objet du délit lorsqu'on se sert de ses nismes automatisés pour modifier et manipuler de nouvelles formes d'avoirs, comme les programmes informatiques et l'information représentant de l'argent.
- Une personne peut se servir de l'ordinateur comme d'un instrument de perpétration ou de planification d'un délit. Un courtier en valeurs a utilisé un ordinateur pour produire de faux états de placements, indiquant des profits considérables, pour tromper ses clients. Il a ainsi volé 53 millions de dollars.
- Une personne pourrait se contenter d'évoquer l'ordinateur pour intimider ou tromper. Le même courtier a dit à ses clients qu'il pouvait réaliser de tels profits sur des ventes rapides d'options d'achat d'actions grâce à un programme informatique secret placé dans ordinateur géant d'une firme de courtage de Wall Street. Le programme n'existait pas et le courtier n'avait même pas accès à l'ordinateur, mais des centaines de clients ont été assez convaincus pour investir au moins 100 000\$ chacun.

Les auteurs de délits informatiques sont habituellement des employés jeunes, hautement motivés, fidèles, et qui n'ont pas de casier judiciaire. Ainsi, des règlements spécifiques sur les délits informatiques exerceraient probablement un plus grand effet dissuasif sur ces individus, qui se considèrent comme des spécialistes particulièrement malins et non comme des voleurs, que sur les criminels professionnels, si l'on voulait faire comprendre aux amateurs la nature criminelle de leur geste. Ils sont convaincus qu'ils ne font de mal à personne, seulement aux ordinateurs. Toutefois, plus en plus de criminels professionnels commettent des délits informatiques, car le milieu type où ils évoluent est de plus en plus envahi par les ordinateurs.

L'évolution des techniques informatiques a donné naissance à un nouveau type de criminel informatique, qui vient remplacer les pirates du téléphone des années 60. Une sérieuse épidémie de vols informatiques se manifeste au pays depuis que les étudiants des écoles secondaires et des collèges apprennent à exploiter un ordinateur et réussissent à avoir accès aux terminaux téléphoniques et aux micro-ordinateurs

de particuliers. Les instructeurs encouragent parfois ces étudiants à s'emparer de techniques, à commettre des fraudes électroniques et à voler les droits de propriété relatifs aux programmes informatiques au moyen de photocopies. D'après un constructeur de programmes informatiques, deux copies sur trois sont utilisées sans avoir été payées, mais leurs profits restent suffisamment importants pour qu'ils ne soient pas touchés par cette question. Nous espérons entreprendre bientôt une grande étude sur ces problèmes qui s'aggravent sans cesse, afin d'évaluer leur importance et de trouver des solutions. Nous croyons que des règlements précis sur les délits informatiques constitueraient un moyen de dissuasion important à cet égard et permettraient de régler ces problèmes.

Il n'existe aucune statistique valable sur le nombre de délits informatiques commis ou sur les pertes que ces actes entraînent. Les nombreux chiffres cités par la presse n'illustrent pas vraiment le problème, car aucun mécanisme acceptable destiné à obtenir des données complètes ou significatives n'a encore été mis au point. Le fait que l'on ne s'entende sur la définition du délit informatique empêche de procéder à une évaluation complète des statistiques. La SRI détient le plus grand nombre d'enregistrements de délits qui correspondent à notre définition; toutefois, plus de 1 000 délits informatiques ont été commis à l'échelle internationale depuis 1958 et ils ne représentent qu'une partie de tous les cas soupçonnés.

Les erreurs et les omissions commises lors de l'exploitation d'un ordinateur entraînent probablement une plus grande perte d'argent que les actes intentionnels. Néanmoins, nous avons réussi à contrôler ces erreurs, dont le coût est inclus dans le traitement des données. Aucun budget n'est prévu ou établi pour les fraudes; ces infractions, une fois décelées, constituent une mauvaise surprise. De plus, le nombre de crimes individuels qui entraînent des pertes considérables a dépassé les pertes accidentelles éprouvées par des particuliers.

Le délit informatique est considéré comme un crime facile. Cette notion est beaucoup trop simpliste et incomplète. Certains délits informatiques, relativement simples, ont été commis en toute sécurité, mais par des personnes qui avaient suffisamment de connaissances, de compétences et de ressources pour le faire, et qui avaient accès à des ordinateurs. Il aurait été difficile pour quelqu'un d'autre d'en faire autant. Certains délits informatiques mineurs ont été commis sans

difficulté par des employés de bureau dotés de connaissances techniques limitées et qui pouvaient facilement avoir accès à un ordinateur; d'autres délits se sont avérés beaucoup plus complexes. Le délit informatique est relativement insensible à l'importance des pertes. Une fois qu'un acte criminel est planifié, il suffit parfois, pour passer de 100 000 dollars à 1 million de dollars d'ajouter trois zéros

Tous les procureurs que j'ai interrogés m'ont affirmé qu'ils ont réussi, ou qu'ils réussiraient, à poursuivre tous les auteurs de délits informatiques au moyen des lois criminelles existantes. Toutefois, bon nombre d'entre eux avouent éprouver de la difficulté à appliquer ces lois à des situations qui n'avaient pas été prévues au moment de leur élaboration, et très peu de procureurs sont conscients des nouveaux crimes qui peuvent être commis et qui ne sont pas visés par les lois actuelles. Le taux de condamnation est très élevé, compte tenu du nombre limité de cas connus. En l'absence de règlements précis sur les délits informatiques, il est plus facile pour les victimes de cacher leurs pertes afin d'éviter l'embarras ou la publicité non sollicitée et pour les procureurs de ne pas intenter de poursuites dans certains cas en raison de leur manque de connaissances en informatique.

L'avenir des délits informatiques

Si l'on se fonde sur des études de cas menées de concert avec les victimes et les enquêteurs, sur des entrevues menées avec plus de 30 contrevenants, et sur des vérifications de sécurité informatique effectuées pour des clients, voici les prévisions que nous formulons:

- Le nombre de délits informatiques augmentera par suite du nombre croissant d'ordinateurs en exploitation et de l'automatisation des activités commerciales.
- Le nombre de certains délits informatiques (paris, distribution et vente de stupéfiants, escroquerie et prostitution) augmentera bien au-delà des quelques cas connus. Les réseaux de transferts électroniques de fonds constituent un moyen intéressant de commettre des fraudes et de soutirer rapidement de l'argent, puis que 400 milliards par jour, sur le plan national, et 600 milliards par jour, sur le plan international, sont transférés entre les ordinateurs des banques et les guichets automatiques. L'utilisation accrue des systèmes de communication des données, des systèmes téléphoniques d'introduction de données, des sorties, du stockage optique des données, des systèmes vidéo et des robots engendreront également de nouvelles formes de délits criminels. Il importe que les règlements criminels soient complets et non liés à la technologie pour éviter que la loi ne devienne très vite périmée.

- L'ampleur, des pertes dans des cas importants augmentera énormément en raison de la concentration des données informatiques dans les ordinateurs et les systèmes de communication, car ces données, étant donné leur fragilité, seront exposées à une puissante manipulation au moyen des ordinateurs. Il suffit de regarder la fraude de 200 millions dont a été victime la Equity Funding Insurance, le détournement de fonds de 21 millions à Los Angeles, le transfert de fonds de 10 millions à Los Angeles, la fraude de 53 millions de titres survenue en Floride, la fraude de 50 millions de marchandises à terme à Denver, et la fraude de 18 millions à Chicago, délits qui ont brisé tous les records de ce type. Certains analystes se sont cependant demandé, ce qui est tout à fait insensé, si ces cas constituent véritablement des délits informatiques, étant donné les diverses définitions qui existent à cet égard. Chacun des 17 Etats dotés de règlements sur le délit informatiques a sa propre définition et, évidemment, aucune loi fédérale n'a encore été promulguée pour régler cette question. Il est clair toutefois que, dans ces cas-ci, l'utilisation des ordinateurs a contribué à créer un milieu spécial, à fournir des outils ainsi qu'à donner l'accès à des ressources financières considérables, alors que les moyens de détection et de prévention étaient limités.
- On peut maintenant beaucoup mieux protéger les opérations informatisées des entreprises qu'à l'époque où les opérations étaient effectuées à la main. On commence à prendre des mesures en ce sens avec les ordinateurs modernes. Les constructeurs d'ordinateurs et les sociétés de réparation offrent aujourd'hui un plus grand nombre de moyens de protection pour satisfaire aux demandes nouvelles et sans cesse croissantes des usagers en matière de sécurité. Bien que les crimes commerciaux et les crimes en col blanc importants diminueront, les difficultés et les risques auxquels devront faire face les auteurs de délits informatiques augmenteront de façon considérable l'importance des pertes dans chaque cas. Cette situation est connue sous le nom d'augmentation des crimes commerciaux.
- L'augmentation des crimes commerciaux peut contribuer à créer de nouvelles situations vulnérables, bien qu'une étude récente effectuée par le groupe de travail de l'American Federation of Information processing Societies démontre qu'en raison de la flexibilité de la société et de sa dépendance limitée à l'égard des ordinateurs, de gros problèmes disparaîtront. Nous croyons que le recours à des moyens techniques comme la cryptographie, les contrôles de gestion avancés, et les codes de conduite découlant, en partie, de règlements criminels sévères, nous pouvons continuer à limiter les risques inhérents à l'utilisation de la technologie informatique et les ramener à un niveau acceptable.

Recommandations

En conclusion, nous recommandons de prendre des mesures législatives établies avec soin pour précipiter l'adoption de lois criminelles fédérales afin de décourager les délits informatiques et de condamner leurs auteurs. Ces mesures devraient porter sur la protection des renseignements, qui constituent des ressources importantes

exposées à des actes criminels commis par des personnes possédant de nouvelles connaissances techniques, et non simplement sur la technologie informatique toujours en évolution. Toutefois, avant que de telles mesures soient adoptées, tous les effets entraînés par les délits informatiques et la législation proposée doivent être identifiés et faire l'objet d'une analyse publique approfondie par une commission d'enquête nationale, afin d'obtenir l'attention et l'appui de ceux dont les intérêts sont en jeu.



If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESS—TÉMOIN

From Gaston, Snow and Ely Bartlett, Palo Alto, California:

Mrs. Susan Nycum, Attorney-at-Law.

De «Gaston, Snow and Ely Bartlett», Palo Alto, Californie:

M^{me} Susan Nycum, Avocate.

HOUSE OF COMMONS

Issue No. 16

Wednesday, June 8, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 16

Le mercredi 8 juin 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the

Thirty-second Parliament, 1980-81-82-83

Première session de la

trrente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

WEDNESDAY, JUNE 8, 1983
(18)

[Text]

The Sub-committee on computer crime met this day at 3:40 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (Etobicoke—Lakeshore).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: From the Canadian Bar Association: Mr. Yves Fortier, President; Mr. Bernard E. Blanchard, Executive Director, Ms. Judith Kingston and Mr. Charles W. MacIntosh, Q.C., of the Standing Committee on Law, Science and Technology.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings and Evidence, Tuesday, March 15, 1983, Issue No. 1.*)

The witnesses made statements and, answered questions.

Ordered,—That the document entitled "Submission to the Sub-committee on computer crime of the Standing Committee on Justice and Legal Affairs by the Law, Science and Technology Committee of the Canadian Bar Association", be printed as an appendix to this day's Minutes of Proceedings and Evidence (*See Appendix "COMP-4"*.)

At 5:36 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

PROCÈS-VERBAL

LE MERCREDI 8 JUIN 1983
(18)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 15h40, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (Etobicoke—Lakeshore).

Aussi présent: M^{me} M. Hébert, chercheuse, Service de la recherche, Bibliothèque du Parlement.

Témoins: De l'Association du Barreau canadien: Me Yves Fortier, président; Me Bernard E. Blanchard, directeur-exécutif; Me Judith Kingston et Me Charles W. MacIntosh, C.R., du Comité permanent sur le droit, sciences et Technologie.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1.*)

Les témoins font des déclarations et répondent aux questions.

Il est ordonné,—Que le document intitulé «Soumission du Comité permanent sur les lois, sciences et technologie, de l'Association du Barreau canadien, au Sous-comité sur les infractions relatives aux ordinateurs du Comité permanent de la justice et des affaires juridiques», soit imprimé en appendice aux procès-verbaux et témoignages de ce jour (*Voir appendice «COMP-4».*)

A 17h36, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

(Recorded by Electronic Apparatus)

[Texte]

Wednesday, June 8, 1983

• 1543

Le président: À l'ordre, s'il vous plaît!

Le Sous-comité reprend l'étude de son ordre de renvoi concernant les infractions relatives aux ordinateurs.

Aujourd'hui comparaissent comme témoins les représentants de l'Association du Barreau canadien à qui je voudrais souhaiter la bienvenue et que je voudrais remercier d'avoir accepté de comparaître devant notre Sous-comité. Je pense que l'expérience et les connaissances de l'Association du Barreau canadien nous aideront beaucoup.

Je demanderais à M. Yves Fortier, président de l'Association du Barreau canadien, de bien vouloir présenter les gens qui l'accompagnent.

M. Yves Fortier (président de l'Association du Barreau canadien): Avec plaisir, madame le président.

Je suis accompagné aujourd'hui de M^{lle} Judith Kingston, de Toronto, de Me Charles W. MacIntosh, C.R., de Halifax, et de M. le bâtonnier Bernard E. Blanchard qui est le directeur exécutif de l'Association du Barreau canadien.

Je vais simplement, si vous me permettez, présenter le mémoire de l'Association en vous disant ces quelques mots. D'abord, il y a quelques mois, nous avons, dans un premier temps, pris connaissance du projet de loi C-667 et nous avons ensuite été mis au courant du mandat qui avait été confié à votre Sous-comité. On a invité le Barreau canadien à se pencher sur ce problème occasionné par l'évolution de l'ordinateur et son impact sur le droit.

So it is with a great deal of enthusiasm that the Canadian Bar Association accepted the invitation of your subcommittee to examine what I would call the "Perri" project, and then, more specifically, the overall area of changes caused in the law by computer technology.

As it happens, the Canadian Bar Association has in place a standing committee on law, science and technology which was set up some years ago and which has been very active at irregular intervals. So, since that body was in place, we turned to that committee and asked if they would do the work with the eventual goal of preparing a brief and submitting it to the members of your subcommittee. They, in turn, asked two of their members, Judy Kingston and Charles MacIntosh, members of the standing committee, to do the work. What you have before you, which has been filed, is a report of a subcommittee composed of both these members of our association and endorsed by the whole Committee on Law, Science and Technology of the Canadian Bar Association. I wish to point out, however, that according to our structure in the Canadian Bar Association, any brief of the association has to go through various levels, various stepping-stones.

TÉMOIGNAGES

(Enregistrement électronique)

[Traduction]

Le mercredi 8 juin 1983

The Chairman: Order, please!

The sub-committee resumes consideration of its terms of reference concerning computer crime.

Today, we have before us as witnesses the representatives of the Canadian Bar Association and I would like to welcome them and thank them for having accepted to appear before our sub-committee. I think that the experience and knowledge of the Canadian Bar Association will be of great help to us.

I would ask Mr. Yves Fortier, President of the Canadian Bar Association to please introduce the people with him.

Mr. Yves Fortier (President of the Canadian Bar Association): With pleasure, Madam Chairwoman.

I am accompanied today by Miss Judith Kingston, from Toronto, Mr. Charles W. MacIntosh, Q.C., from Halifax and Mr. Bernard E. Blanchard who is Executive Director of the Canadian Bar Association.

If you do not mind, I will simply present to you the Association's brief in a few words. First of all, a few months ago, we examined Bill C-667 and were then apprised of the mandate that was given your sub-committee. The Canadian Bar was invited to examine the problem posed by the evolution of the computer and its impact on law.

Donc, c'est avec beaucoup d'enthousiasme que l'Association du Barreau canadien a accepté l'invitation lancée par votre sous-comité d'étudier ce que j'appellerais le projet «Perri» et ensuite, plus précisément, tout le domaine des changements apportés au droit par cette question de l'ordinateur.

Comme par hasard, l'Association du Barreau canadien avait mis en place il y a quelques années déjà, un comité permanent sur le droit, la science et la technologie qui a siégé à des intervalles irréguliers. Puisque ce comité existait déjà, nous avons demandé à ses membres de faire un certain travail dont le but éventuel serait de préparer un mémoire à présenter aux membres de votre sous-comité. À son tour, ce comité a demandé à deux de ses membres, Judy Kingston et Charles MacIntosh, membres du comité permanent, de faire ce travail. Ce que vous avez devant vous, ce qui a été déposé, est un rapport émanant d'un sous-comité composé de ces deux membres de notre association et entériné par le comité sur le droit, la science et la technologie de l'Association du Barreau canadien. J'aimerais cependant souligner qu'à cause des niveaux hiérarchiques qui existent au sein de l'Association du Barreau canadien, tout mémoire émanant de l'Association doit être approuvé à divers niveaux.

[Texte]

• 1545

Dans le cas qui nous occupe présentement, à cause des courts délais, le mémoire n'a pas suivi le cheminement habituel. Donc, le Comité sur la législation et la réforme du droit ne s'est pas penché sur le mémoire, pas plus que la section de la justice criminelle. La section du droit criminel a, évidemment, un intérêt bien spécifique et bien arrêté pour cette question-là.

C'est avec ces mises en garde, si vous me le permettez, madame le président, qu'il nous fait plaisir aujourd'hui de vous livrer ce mémoire de notre comité du Barreau canadien. Je vous répète qu'il n'a pas été approuvé par l'Association comme telle, mais ce sont les experts qui parlent, néanmoins.

So the brief is divided into two parts. In the first part, which starts on page 1, we address the Hon. Perrin Beatty's Bill C-667. In the second part, which starts on page 6, we discuss how the concerns which are created in our minds by Bill C-667 could be met with what we qualify as alternate solutions.

So without further ado, Madam Chairman, and with your permission, I would like to ask Miss Kingston to speak to the first portion. Mr. MacIntosh will speak to the second portion, and then all of us will be prepared to answer your questions.

Thank you.

The Chairman *Merci.*

Madam Kingston.

Ms Judith Kingston (Member, Standing Committee on Law, Science and Technology, Canadian Bar Association): *Merci.*

As we are all aware, rumours have been spread among people, in newspapers and in magazines, that a thing called "computer crime" has been spreading. This has caused great concern in society, because they feel computer crime, or what is reported in the rumours to be computer crime, has not been met by our present Criminal Code. This has caused the Hon. Perrin Beatty to introduce a bill, called Bill C-667, to meet those concerns. I would like to discuss now some of the items that have been addressed by the Hon. Perrin Beatty in this bill.

The first item I would like to address is the explanatory note found on page 1a of Perrin Beatty's bill. Do you all have a copy of his bill? Yes, fine.

The first concern is raised in the explanatory notes. He stated that the purpose of the bill was to address various issues that have been related to computer use and abuse, which have prevented the courts from coming to grips with this whole area.

We have had some reported cases in Canada that reportedly are concerned with computer crime. One of these cases was *R. v. McLaughlin* in Alberta. This case basically held that it was not theft of computer services, because it was use of a telecommunications facility, which is different from a computer facility.

[Traduction]

In this case, however, the brief did not follow the usual path. Therefore, the committee on Legislation and Law Reform did not look at the brief nor did the section concerned with criminal justice. The criminal justice section, of course, has a very specific and definite interest in that question.

So, armed with those warnings, if you do not mind, Madam Chairwoman, it is with great pleasure that we are giving you today this brief from this committee of ours. I would like to repeat that it has not been approved by the association itself but these are experts speaking, nonetheless.

Le mémoire se divise donc en deux parties. La première partie qui débute à la page 1 porte sur le bill C-667 de l'honorable Perrin Beatty. La deuxième partie qui débute à la page 6 est consacrée aux problèmes créés, selon nous, par le projet de loi C-667 et que l'on pourrait régler grâce à des solutions de rechange.

Donc, sans plus tarder, madame le président, et avec votre permission, j'aimerais demander à M^{lle} Kingston de vous parler de la première partie. M. MacIntosh vous parlera ensuite de la deuxième et nous serons alors tous prêts à répondre à vos questions.

Merci.

Le président *Thank you.*

Madame Kingston.

Mlle Judith Kingston (membre, Comité permanent sur le droit, la science et la technologie, Association du barreau canadien): *Thank you.*

Comme nous le savons tous, la rumeur s'étend chez tous, véhiculée par les journaux et les revues, que la «truaudique» s'installe de plus en plus. Voilà qui inquiète beaucoup la société car l'on y croit que notre Code criminel actuel ne peut rien faire pour punir les fautifs dans ce domaine. Voilà pourquoi l'honorable Perrin Beatty a présenté son projet de loi C-667. J'aimerais maintenant vous dire quelques mots à ce propos.

Tout d'abord, voyons la note explicative qui se trouve à la page 1a de ce projet de loi. Vous en avez tous un exemplaire? Bon, parfait.

Le premier problème est soulevé dans les notes explicatives. Il y précise que le projet de loi vise à résoudre certains problèmes entourant l'emploi des ordinateurs qui, traditionnellement, ont empêché les tribunaux de s'attaquer au crime dans le domaine des ordinateurs.

Il y a eu certains cas devant les tribunaux au Canada à ce propos. Un de ces cas était celui de *R. c. McLaughlin* en Alberta. Dans ce cas, fondamentalement, ce qui a été dit, c'est qu'il ne s'agissait pas du vol de services d'ordinateur car il s'agissait de l'utilisation de matériel de télécommunications, ce qui est fort différent d'une installation d'informatique.

[Text]

The issue raised in this case of *R. v. McLaughlin* has not been met in the Honourable Mr. Beatty's bill, and we raise that in our first comments dealing with Bill C-667. This seems to be an area that has caused some concern with the data-processing community, because they feel someone could use their computer facility without altering or destroying their programs or without stealing data, yet still take something of value to them; and that is computer time. It is an intangible. It is not property as presently defined in the Criminal Code; and those in the data-processing community to whom I have talked feel this concern should be addressed.

• 1550

What I understand from Mr. Beatty's notes from his address of June 8, 1982, before the Ontario Universities' Computing Conference at the University of Guelph—he felt that he did not have to address this issue, because if you were to access someone's computer system, to paraphrase him, you would have to use their software or tamper with their data, or do something once you are in there, and he felt, addressing those concerns, that what you do once you are in the system will cover anybody who accesses the computer time.

So he felt that you did not have to have a specific section dealing with computer time, just a section dealing with what they do once they have the access to computer time. The data-processing community feels that is not adequate, because you could use someone's computer time without using their software and without damaging their data.

About the specific clauses in the bill, we are only dealing with the five clauses in the bill that deal with computer crime, we are not dealing with Clause 6, which deals with the Canada Evidence Act.

The first clause in Bill C-667 defines a computer. We have addressed this concern on page 2 of our report. We feel that the first problem with any definition of a computer is that it is going to have to be so broad in order to include future technology that it will encompass very many things that you do not really want it to encompass. I assume that was in Mr. Beatty's mind when he drafted Clause 1, because he excluded things like a hand-held calculator or similar device, realizing that he had a fairly broad definition. However, I think the definition may still be a little too broad.

The other problem with defining a computer is in making it so narrow that the definition by itself excludes things like hand-held computers and player pianos. The problem there is that if you draft it so it is too narrow, you will not be able to take into account the future technology, because the narrow definition will not be broad enough in scope.

However, regardless of which way you define a computer system we still felt that Clause 1 was not necessary, as "computer" by itself was not directly used in the bill. It was indirectly used in the bill in three places. One was where he referred to computer software; the second was where he referred to computer data; and the third was where he referred

[Translation]

Le problème soulevé dans le cas de *R. c. McLaughlin* n'est pas réglé par le projet de loi de l'honorable M. Beatty et nous le soulignons dans nos premiers commentaires. Ce domaine semble poser de sérieux problèmes chez ceux qui s'intéressent aux ordinateurs car ils croient que quelqu'un pourrait se servir de son ordinateur sans altérer ou détruire les programmes ou sans voler de données, mais tout en y prenant quelque chose qui a une certaine valeur, c'est-à-dire le temps de l'ordinateur. C'est quelque chose d'intangible. D'après les définitions données au Code criminel, il ne s'agit pas de propriété; tous ceux à qui j'en ai parlé et qui s'intéressent aux ordinateurs de près ou de loin croient qu'on devrait s'attaquer à ce problème.

Le 8 juin 1982, M. Beatty présentait un exposé à l'Université de Guelph, à l'occasion de la Conférence sur l'informatique, parrainée par les universités ontariennes. Je me suis reporté à cet exposé et si j'ai bien compris, il n'a pas abordé cette question parce que si l'on a accès à un ordinateur appartenant à quelqu'un d'autre, il faut en utiliser le logiciel ou se servir des données qu'il contient; voilà pourquoi il estimait que le fait même de se servir d'un ordinateur qui appartient à quelqu'un d'autre, tiendrait compte de l'utilisation frauduleuse du temps d'ordinateur.

Voilà pourquoi M. Beatty estimait qu'il n'était pas nécessaire de prévoir un article particulier concernant le temps d'ordinateur, mais tout simplement les infractions possibles une fois que quelqu'un a accès à l'ordinateur. Les informaticiens estiment que cela ne suffit pas, car on peut se servir du temps d'ordinateur de quelqu'un sans toucher au logiciel, sans faire de dégât aux données.

Nous n'avons étudié que cinq articles du projet de loi, c'est-à-dire ceux qui ont trait aux infractions relatives aux ordinateurs, et nous avons laissé de côté l'article 6, qui porte sur la Loi sur la preuve au Canada.

Le premier article du Bill C-667 définit ce qu'est un ordinateur. Nous développons cela à la page 2 de notre mémoire. Le problème majeur que pose toute définition d'un ordinateur est qu'il faut qu'elle soit assez vaste pour inclure tout autre développement technologique, mais alors elle inclut toutes sortes de choses qui n'ont rien à voir. Je suppose que M. Beatty était très conscient de cela quand il a rédigé l'article 1, car il a exclu les calculateurs ou autres petits appareils ou dispositifs semblables, l'énoncé de sa définition étant très vaste. Toutefois, il l'est peut-être encore trop.

Mais le problème inverse se pose. On peut offrir une définition assez étroite d'ordinateur qui du fait même exclura les petits calculateurs et les pianos mécaniques. Mais dans un tel cas, on ne pourra pas y englober les développements futurs.

Néanmoins, quelle que soit la définition que l'on donne du mot ordinateur, nous estimons que l'article 1 est superflu, car les autres dispositions du projet de loi n'utilisent pas le mot «ordinateur» seul. En effet, le mot est utilisé indirectement à trois reprises. On parle de logiciel d'ordinateur, de données d'ordinateur et de données informatisées. Il n'est pas besoin de

[Texte]

to computerized data. We felt that you did not need a definition of a computer to define what the first word in all those definitions meant. If you were to have a definition at all, maybe you should define computer software; not just computer, but computer software or computer data or computerized data. But we felt that Clause 1 was not necessary.

Clause 2 of the bill expanded the definition of property, and it included computer software or programs, copies thereof, retrievable computer data or information produced and stored in machine-readable form by any means.

We had several concerns with that definition, which expanded part of the definition. The first problem, which we have raised on page 3 of our report, is about the first words in that expanded definition, "computer software or programs".

We first of all could not understand why a distinction was made between computer software and programs, and if there was a distinction, what it was. The second problem we had is that we were unsure whether or not that would include technology such as firmware. "Firmware" is a term used to refer to instructions contained in read-only memory and which works with the operating system to control the computer system. It is actually hard-core programs or software, whatever term you want to use for it; but instructions. On reflection on the words "computer software or programs", we were unsure whether or not they included that. So we felt that those two words were unclear and needed more precise drafting.

We were also unsure on the next words, what "copies thereof" would mean. You can write a program on a piece of paper and you could make a copy of that program on magnetic media. If you were to have a case involving a copy from paper onto magnetic media, it is unclear whether or not that magnetic medium would be a copy of the program that was on paper, because it is in another form. It may not be a copy. We were unsure what "copies thereof" meant.

• 1555

The next words in the definition we were concerned with were "retrievable computer data or information". We were once again unsure of the distinction between computer data and information. If a distinction was to be made, what is the difference? I have no idea what the difference is. If there is no distinction, why have both "computer data" and "information" in the definition? I think it is going to lead to confusion later on in the courts.

We had a further problem with those words "retrievable computer data or information". We were not sure why "retrievable" was used. If the computer data is not retrievable, then we thought it might be difficult for someone to be able to do any act that would be termed a criminal act on it. So if the data is not retrievable, then why have "retrievable" in the

[Traduction]

définir «ordinateur» pour définir l'expression entière. Si donc on tient à donner des définitions, il faudrait se borner à définir logiciel d'ordinateur, données d'ordinateur et données informatisées. Voilà pourquoi nous pensons que l'article 1 est superflu.

L'article 2 du projet de loi redéfinit le mot «biens», pour inclure désormais logiciel d'ordinateur, programme d'ordinateur, copies de logiciels ou de programme d'ordinateur, ainsi que l'information entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé.

Cette définition ne nous satisfait pas pleinement tout d'abord pour la raison que nous soulevons à la page 3 de notre mémoire. C'est l'utilisation des mots «logiciels ou programmes d'ordinateur» dans cette définition élargie qui pose un problème.

Nous ne comprenons pas pourquoi on fait une distinction entre logiciels d'ordinateur et programmes d'ordinateur, et si de fait il y a une distinction, nous voudrions la connaître. Deuxièmement, nous ne savons pas si une telle définition engloberait le relationnel. Le «relationnel» est un terme utilisé pour décrire les instructions contenues dans une mémoire fixe dont on se sert en même temps que les autres commandes de contrôle de l'ordinateur. En fait, il s'agit bien de programmes, de logiciels, mais ce sont des instructions. Voilà pourquoi on s'est demandé si la définition offerte pour les expressions «logiciels ou programmes d'ordinateur» tenait compte de ces instructions. Voilà pourquoi nous recommandons un libellé plus clair.

Nous ne comprenons pas non plus l'utilisation de l'expression «les copies de logiciels ou programmes d'ordinateur». On peut écrire un programme sur une pièce de papier et on peut le mettre aussi sur mémoire magnétique. S'il y avait donc un cas où la copie aurait été faite à partir d'une copie sur papier sur support magnétique, on peut se demander si le support magnétique pourrait véritablement être considéré comme une copie du programme sur papier, le support étant différent dans les deux cas. Il se peut qu'il ne s'agisse pas d'une copie. Nous ne sommes donc pas sûrs de la signification de «copie de logiciels ou programmes d'ordinateurs».

En outre, dans la définition, nous nous posons des questions sur la signification de «information...repérable par ordinateur». Nous ne sommes pas sûrs de la distinction que l'on fait en anglais entre «données d'ordinateurs» et «information». S'il y a une distinction, quelle est-elle? Je n'en vois pas. Il n'y a pas de distinction, pourquoi utiliser les deux expressions? Je pense que cela prêterait à équivoque devant les tribunaux.

D'autre part, ces expressions nous causent un autre souci. En effet, pourquoi a-t-on utilisé le mot «repérable». Si une information n'est pas repérable, il serait difficile à quiconque de commettre une infraction que l'on qualifierait de criminelle. Si donc l'information n'est pas repérable, pourquoi spécifier «repérable» dans la définition? Nous ne sommes pas sûrs de la signification de ce mot.

[Text]

definition? We were not sure what the meaning of that word was there.

We also had a problem with the words "produced and stored in machine-readable form". There is now technology on the market today—and who knows what will be in the future—the technology today does allow voice transmission. It allows laser beams to pick up writing. It does not necessarily have to be keyed into a computer terminal, or it does not necessarily have to be encoded in magnetic media to be machine-readable. So we are not sure whether "produced and stored in machine-readable form" would include something like this conversation, or what necessarily it does mean.

Conversely, if "machine-readable form" were to have a narrow definition, depending on what the courts might decide, then we were unsure whether or not "produced and stored in machine-readable form" would be broad enough, given the fact that a lot of data is initially produced on a piece of paper. For example, Chargex slips initially are produced on the slip you get in a store. That is how they are produced. They are then later transcribed into something that if it is machine-readable, to take a narrow definition, is then transcribed onto punched cards or tape or disc form. I am not sure whether "produced and stored in machine-readable form" would necessarily catch that. Maybe it would catch only things that are produced, i.e. keyed, right in from a terminal—the original form keyed into a computer terminal. Then it is produced and stored in machine-readable form. But does "produced" mean originally produced, or does it mean transcribed from an original record into machine-readable form? We were very unclear as to what that meant.

The next clause we had concern with was clause 3 of the bill. This clause creates a new offence of theft. In a very general sense it creates a new offence of theft if you without colour of right, or fraudulently, divert to your own use or the use of another person all or part of a computer program or copy thereof or any computerized data.

We had some concerns with this clause as well. One of our first concerns was the use of the word "divert". We were very unclear on what "divert" would mean and how you would argue that in any litigation or entered case.

With computer technology it is very possible to have a computer system spread across international boundaries. Would "divert" happen when you actually changed the flow of something to come your way, which probably it could mean? For example, if I had a terminal in Toronto and I wanted to get information in Buffalo, when I key into my terminal here, I am not diverting anything yet. I do not divert it until I tap into the system in Buffalo and actually change the flow of where that information is going, to be sent back up through my terminal so I can receive it. So possibly you could argue—it is unclear, but possibly you could argue—that the "divert" aspect of this offence would take place in Buffalo, where you

[Translation]

En outre, les mots «entrée sous une forme repérable par ordinateur et emmagasinée» nous laissent perplexes. La technologie permet aujourd'hui, et qui sait ce qu'elle permettra demain, la transmission de la voix. Elle permet à des rayons laser de lire des textes. Il n'est pas nécessaire que des renseignements soient mis sur ordinateur ou encodés sur support magnétique pour être repérables par ordinateur. Nous ne sommes donc pas sûrs que l'expression «entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé» incluerait notre conversation par exemple, et nous ne savons pas ce que cela signifie.

D'autre part, si l'on donnait à l'expression «repérable par ordinateur» une définition étroite, après interprétation des tribunaux, nous ne sommes pas sûrs non plus que la définition de «entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé» serait assez large, car beaucoup de données subissent une première entrée sur une feuille de papier. Par exemple, les factures Chargex sont tout d'abord des factures que l'on donne au magasin. Il y a d'abord une entrée là. Ensuite, elles sont transcrites sous une forme repérable par ordinateur, si l'on prend la définition étroite des termes, car elles sont mises sur carte perforée, sur une bande ou un disque. Je ne sais pas si l'expression utilisée ici tiendrait compte de cela. Cette expression ne tiendrait compte que de ce qui est perforé, à partir d'un terminal. En effet, ces factures sont ensuite entrées sous une forme repérable par ordinateur et emmagasinées sur un enregistrement informatisé. Et quand on dit «entrée», est-ce qu'on parle de la première entrée, ou est-ce qu'on parle de la transcription de la facture originale sous une forme repérable par ordinateur. Nous ne sommes pas sûrs de ce que cela signifie.

Passons à l'article 3 du bill. Cet article crée une nouvelle infraction criminelle, un vol. En effet, vous commettez une nouvelle infraction criminelle si sans apparence de droit, ou frauduleusement, vous détournez à votre propre usage ou à l'usage d'une autre personne tout ou partie d'un logiciel, ou copie de logiciel, ou toute information mise en oeuvre sur ordinateur.

Nous nous posons des questions au sujet de cet article. Tout d'abord l'utilisation du mot «détourne». Nous ne savons pas ce que «détourne» signifie et quelle serait l'argumentation présentée.

La technologie des ordinateurs permet que le réseau s'étende au-delà des frontières internationales. Est-ce qu'on pourrait parler de «détourner» quand on modifierait le cours des renseignements à son propre usage? Par exemple, si j'avais un terminal à Toronto et que je voulais obtenir des renseignements à Buffalo, le fait de donner les commandes ici ne constitue pas un détournement. Il n'y a pas détournement tant que je n'ai pas rejoint Buffalo, et que je n'ai pas changé le cours des renseignements, c'est-à-dire tant que je ne les ai pas acheminés pour les recevoir à mon terminal. On pourrait donc prétendre que le «détournement» a lieu à Buffalo dans ce cas-là, car c'est là qu'on a changé le cours des renseignements.

[Texte]

change where the information was to flow; in which case we might have problems prosecuting under this proposed section.

• 1600

We thought what might possibly aid in any kind of prosecution is to create a new section similar to Section 301.1(2) of the present Criminal Code, which talks about credit cards. Basically, this proposed section states if you have committed an offence anywhere which, if it had been committed in Canada, would have been a criminal offence, you can be prosecuted for it with respect to a credit card offence under Section 301.1. Due to the unclear meaning of the word "divert" and due to the state of the art in technology, where it is very easy for computer technology to go across international boundaries, we felt you would need a section similar to Section 301.1(2) with respect not only to Clause 3 of the bill but also to Clause 5 of the bill, which amends the mischief sections, successfully to prosecute any offence that may be created.

We also had a problem in this clause with respect to the use of the words: "computer program or copy thereof or any computerized data". First, we are unsure why the definition, which was drafted in Clause 2 of the bill, was not also incorporated in Clause 3 of the bill. Why did he not refer to:

... computer software or programs, copies thereof, and retrievable computer data or information produced and stored in machine-readable form by any means ...

Why was it shortened to be just: "computer program or copy thereof or any computerized data"?

We were unsure why there was a shortened form of the definition of property, as set out in Clause 2, that was not used in Clause 3, and if so, what the relevance of the distinction is. We were also unsure what the difference was between computer data, used in Clause 2 of the bill, and computerized data, used in Clause 3 of the bill. These were all terms we were very unsure of and thought could lead to great confusion in the courts.

Our next concern was with Clause 4 of the bill. Clause 4 of the bill proposes to amend the definition of property used in the present Section 385 of the Criminal Code. This definition used in Clause 4 of the bill is very similar to the expanded relevant part of Clause 2 of the bill about the computer software programs. Therefore our comments with respect to Clause 2 of the bill would apply equally to Clause 4 of the bill.

Our last comments are about Clause 5 of the bill. Clause 5 of the bill amends the mischief section as presently found in Section 387 of the Criminal Code. In effect, the main amendment in the bill comes in proposed Section 387.(1)(c). It was amended to include:

[Traduction]

Dans un tel cas, on pourrait avoir du mal à invoquer l'article proposé devant le tribunal.

A notre avis, on pourrait peut-être faciliter ce genre de poursuites en créant un nouvel article semblable à l'article 301.1(2) de l'actuel Code criminel, qui porte sur les cartes de crédit. En substance, cet article prévoit que, si vous avez commis à l'étranger une infraction qui, si elle avait été commise au Canada, aurait été une infraction criminelle, vous êtes passible de poursuites en ce qui concerne les délits liés aux cartes de crédit. Étant donné que le sens du mot «détourner» n'est pas clair et que les progrès technologiques permettent facilement de faire traverser les frontières à des circuits informatiques, nous estimons qu'il serait nécessaire d'avoir un article semblable à l'article 301.1(2), en ce qui concerne non seulement l'article 3 du projet de loi, mais également l'article 5, lequel modifie les articles portant sur les méfaits, si l'on veut réellement pouvoir poursuivre les infractions qui en résultent.

Nous avons par ailleurs des réserves à l'égard du libellé de cet article, et plus précisément à l'égard de l'expression suivante: «logiciel ou copie de logiciel, ou toute information mise en oeuvre sur ordinateur». Tout d'abord, nous ne comprenons pas pourquoi la définition que contient l'article 2 du bill, n'a pas été également incorporée à l'article 3. Ainsi, pourquoi ce dernier ne reprend-il pas la même définition, ce qui donnerait:

... les logiciels ou programmes d'ordinateur, les copies de logiciels ou programmes d'ordinateur, et l'information entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé ...

Pourquoi avez-vous raccourci ce libellé pour le limiter simplement à «logiciel, ou copie de logiciel, ou toute information mise en oeuvre sur ordinateur»?

Nous ne comprenons pas non plus pourquoi l'on a choisi une définition tronquée du mot «bien», de sorte que celle qui figure dans l'article 2 n'est pas reprise dans l'article 3. Si c'est délibéré, nous aimerions savoir quelle distinction il faut faire entre les deux. Nous ne savons pas non plus très bien quelle différence existe entre l'information entrée sur ordinateur, dont il est question à l'article 2, et «l'information mise en oeuvre sur ordinateur», dont il est question à l'article 3. Tous ces termes et expressions ne nous paraissent pas très clairs et risquent donc, à notre avis, de jeter la confusion dans les tribunaux.

Passons maintenant à l'article 4 du projet de loi. Cet article propose de modifier la définition de «bien» que contient l'actuel article 385 du Code criminel. La définition proposée à l'article 4 du projet de loi se rapproche beaucoup de la partie correspondante de l'article 2 du bill, qui porte sur les programmes de logiciel. En conséquence, les observations que nous avons faites au sujet de l'article 2 valent également pour l'article 4.

Pour terminer, passons à l'article 5. Cet article modifie l'article 387 du Code criminel, qui porte sur les méfaits. Le principal amendement du bill figure dans le projet d'article 387.(1)(c). En effet, cet alinéa a été modifié afin d'inclure:

[Text]

387.(1) Every one commits mischief who wilfully
(c) and without authorization, express or implied, destroys or damages a computer program or computer data or alters a computer program or computer data in a way that renders it useless or inoperative or diminishes its commercial or scientific value,

We had some concerns with this part of Clause 5 of the bill. Our first concern was about the words "computer program or computer data". Once again, as we discussed about Clause 3 of the bill, we were unsure why a shortened form of the definition that was found in Clause 4 of the bill is now being incorporated into Clause 5. If there is to be some relevant distinction made between the expanded definition in Clause 4 and the shortened version used in proposed Section 387.(1)(c), then I think it should be explained in a manner that is much clearer. I think this could lead to great confusion. It drops out the word "software". We were not sure of the distinction between computer program and software anyway; but if there is a distinction, it is dropped in proposed Section 387.(1)(c) and we are not sure why.

Once again, in "computer data", the word "information" was deleted.

• 1605

Our next concern is about the word "renders". We are not sure what "renders" means. Does "renders" mean that the destruction or damage must take place at the same time that the data or the program is made useless, inoperative or diminished in its commercial or scientific value, or can there be some time-lag between them? For example, in present technology I am sure we have all read stories in magazines and newspapers about how some programmers can draft and imbed software time bombs—imbedded in the code—that are to take effect later on in the future, on some specific date; or if some specific occurrence happens the whole thing will destruct or something will happen. Would the word "renders" catch that? Does the word "renders" take into account the fact that there can be destruction or damage that happens later? We were very unclear as to that word.

We were also unclear as to what the words "diminishes its commercial or scientific value" were to mean. On reading that we felt that it would probably not include computer programs or computer data that were used for personal enjoyment or that were not created for the purpose of profit, even though they might have been created by a commercial institution, or were not created for scientific purposes.

We thought those words should be clarified. Particularly, a commercial enterprise may create—and I know presently many of them do create—many programs and a lot of data that it never intends to sell to the public, particularly any competitor; they are created for internal purposes only. They may have no scientific value, just business value, and no commercial value because they are not intended to go out to the public. I am not sure whether these words would include an

[Translation]

387.(1) Commet un méfait, quiconque, volontairement,
c) et sans autorisation, ni expresse ni tacite, endommage ou détruit un logiciel d'ordinateur ou de l'information mise sur ordinateur, ou les modifie de sorte qu'ils deviennent l'un ou l'autre inutiles ou inopérants ou que leur valeur commerciale ou scientifique est diminuée,

Cet alinéa de l'article 5 nous pose des problèmes, tout d'abord en ce qui concerne l'expression «logiciel d'ordinateur ou de l'information mise sur ordinateur». Comme pour l'article 3 précédent, nous ne comprenons pas pourquoi l'on a inclus dans l'article 5 une forme abrégée de la définition que contient l'article 4. S'il faut faire une distinction justifiée entre les deux, c'est-à-dire entre la définition élargie de l'article 4 et la version abrégée de l'article 387.(1)c), il faudrait que ce soit expliqué de façon beaucoup plus claire, sinon on risque de provoquer une grande confusion. Dans la deuxième définition, il n'est plus question de «logiciel», mais je dois dire que, de toute façon, nous ne savons pas s'il faut faire une distinction entre un programme d'ordinateur et un logiciel; toutefois, s'il y en a une, elle n'existe plus dans l'article 387.(1)c) et nous ne comprenons pas pourquoi.

Ici encore, lorsqu'on emploie l'expression «information mise sur ordinateur» on ne reprend pas le mot «information» dans la version anglaise.

Parlons maintenant du terme «rend». Que veut-il dire exactement? Cela signifie-t-il que la destruction ou la détérioration doit se produire au même moment où le logiciel a été rendu inutile ou inopérant, ou que sa valeur commerciale ou scientifique a été diminuée, ou bien y a-t-il un délai entre les deux actes? Par exemple, avec la technologie actuelle, nous savons tous, nous l'avons lu dans les journaux, que les programmeurs peuvent concevoir et entrer dans le logiciel «des véritables bombes à retardement» qui font effet à une date ultérieure; de même, si un autre fait précis se produit, tout est détruit ou détérioré. Le terme «rend» englobe-t-il tous ces cas-là? Tient-il compte du fait que la destruction ou la détérioration peut se produire plus tard? Ce terme ne nous semble pas très clair.

Nous ne comprenons pas non plus exactement ce que veut dire l'expression «ou que leur valeur commerciale ou scientifique ait diminué». À notre avis, une telle expression n'incluerait sans doute pas les programmes d'ordinateurs ou les informations mises sur ordinateur, destinés à un pur plaisir personnel ou n'ayant pas été créés dans le but de faire des profits, même s'ils ont été mis au point par une entreprise commerciale, ou encore n'ayant pas été créés à des fins scientifiques.

Nous estimons que ces termes devraient être précisés. En effet, une entreprise commerciale pourrait mettre au point, et je sais que bon nombre d'entre elles le font déjà, des programmes et des informations qu'elle n'a jamais l'intention de vendre au public, et encore moins à un concurrent; ces programmes sont donc mis au point pour un usage interne uniquement. Ils servent donc uniquement à l'entreprise et ne peuvent avoir aucune valeur scientifique ou commerciale étant donné qu'ils

[Texte]

offence about the destruction of, or damage to, such kinds of computer data or computer programs.

Those are our thoughts. Thank you.

The Chairman: Mr. MacIntosh would like to deal with the other section and then Mr. Beatty can comment on your comments. He will defend his bill and will discuss the issue.

Mr. Charles W. MacIntosh (Member, Standing Committee on Law, Science and Technology, Canadian Bar Association): Before moving on to part II, I have one remark about the Canada Evidence Act proposal contained in Mr. Beatty's bill. I should point out that the Canadian Bar Association will be making a more formal presentation about the proposed Canada Evidence Act dealing with this same topic, and anything I say is not to be taken as contrary to what they are going to say. It appears that another way this problem could be dealt with, which we submit might cover a broader area than just computer, would be a new definition of the word "record". As it is now found in the Canada Evidence Act, it deals peripherally with this type of subject. Could I suggest the following definition for "record"?

"Record" means any information set down in handwriting, drawing, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other manner of setting down information for the purpose of data compilation and storage, and includes a printout from a computer or similar device in a form which may be understood whether the printout is the result of a process of data retrieval or a replica of data stored.

We feel that that definition includes material coming out of the computer that is stored in the computer—that is, the same information as is put in is taken out—and also material where the computer reworks other data to come up with a different answer, which the present definition, we submit, does not do.

• 1610

The second part of our brief deals with the suggested draft clause which is found on the last page, and attempts to justify those provisions. I may say that we are in support of the intent of the legislation and would like to see the matter drafted in such a way that the courts could not be misled as to that intent, as is often the problem with technological matters when they come before our courts.

We feel "computer" can be defined in the context of other definitions of computer-related material. We have examined the Arizona and Florida acts, the model computer crime bill and the Illinois legislation, and our recommendation for a definition for a computer in this context is "A computer means an internally programmed general-purpose device capable of automatically accepting data, processing data, and supplying

[Traduction]

ne sont pas destinés à être commercialisés. Je ne sais pas si les termes employés ici incluraient le délit d'infraction de détérioration d'informations ou de programmes d'ordinateurs.

Voilà donc ce que nous en pensons. Merci.

Le président: Lorsque M. MacIntosh aura traité de l'autre partie de votre exposé, M. Beatty pourra vous dire ce qu'il pense de vos commentaires. Je suppose qu'il ne manquera pas de défendre son projet de loi.

M. Charles W. MacIntosh (membre du Comité permanent sur le droit, la science et la technologie, Association du Barreau canadien): Avant de passer à la deuxième partie de notre rapport, j'aimerais faire une remarque au sujet de la proposition que contient le bill de M. Beatty au sujet de la Loi sur la preuve au Canada. Permettez-moi de vous signaler que l'Association du Barreau canadien a l'intention de présenter un mémoire plus officiel au sujet du projet de loi sur la preuve, et tout ce que je dis ne doit pas être interprété à l'encontre de ce que nos représentants auront à dire plus tard. Une autre façon d'aborder le problème, et qui permettrait à notre avis de ne pas se limiter aux ordinateurs, consisterait à adopter une nouvelle définition du mot «dossier». Le texte actuel de la Loi sur la preuve du Canada ne traite de ce sujet que de façon très périphérique. Puis-je donc vous proposer la définition suivante pour le terme «dossier»?

«Dossier» signifie toute information consignée par écrit, par dessin, par dactylographie, par impression, par photocopie, par photographie, par impulsion magnétique, par enregistrement mécanique ou électronique, ou par tout autre moyen utilisé pour compiler et emmagasiner des informations, et cela inclut également les imprimés d'ordinateurs, ou tout dispositif similaire, que cet imprimé soit l'aboutissement d'un exercice de repérage ou de duplication des données emmagasinées.

Nous estimons que cette définition englobe toutes les informations sortant de l'ordinateur après y avoir été emmagasinées, ainsi que les autres documents produits par l'ordinateur à partir de ces données emmagasinées. Par contre, la définition actuelle ne permet pas de le faire.

La seconde partie de notre exposé contient les projets d'amendement que nous vous soumettons en dernière page, ainsi que les justifications de ces amendements. Permettez-moi de vous dire que nous approuvons l'objet de ce projet de loi, mais que nous estimons que son libellé ne doit pas comporter le risque d'être mal interprété par les tribunaux, comme cela arrive souvent lorsque des affaires très techniques leur sont soumises.

Nous estimons que le terme «ordinateur» peut être défini dans le contexte d'autres définitions de matériel connexe. Nous avons étudié les lois de l'Arizona et de la Floride, ainsi que le projet de loi de l'Illinois, et nous recommandons la définition suivante: «Un ordinateur est un dispositif d'application générale, qui a été programmé et qui est capable d'accepter automatiquement des données, afin de les traiter et de fournir le résultat de l'opération». Vous constaterez que cette défini-

[Text]

the result of the operation". You will note that this definition describes the computer by what it does rather than what it is.

Our second point is that we feel not only the computer itself should be protected but also the peripherals and the other equipment attached to a computer, as well as telecommunication devices, when they are being used in conjunction therewith. On the top of page 9 we have suggested the definition of a computer network.

In addition to hardware, we feel that software should also receive protection. The State of Michigan uses two definitions to achieve this, which we feel should be seriously considered. The first is a definition of a computer program: it means a series of instructions or statements which are in a form acceptable to a computer and which permit the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

A definition of computer software: a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

A computer system: a set of related connected or unconnected computer equipment devices and software.

About the solution from the hon. member, Mr. Beatty, by amending the mischief section to provide a cover-all about computer crime, we suggest that this may be trivializing the importance of computer crime. As you have already heard numerous briefs on this topic, I do not intend to go over that in great detail. The subject-matter is dealt with in our written brief.

We do see, however, that computer crime can be very serious and can result in train wrecks and aircraft crashes, and millions and millions of dollars being stolen; or, on the other hand, it may be a student prank and nobody is harmed at all, except that obscene words appear on the screen when they should not. So it can be a very serious thing; on the other hand, it can be a matter of mischief in the true sense of the word. The word "mischief" appears to be associated in the public mind with smashed windows, school desks being burned and car aerials being stolen. We feel that computer crime is just too serious a matter to be dealt with under this clause.

When it comes to the matter of penalty, this broad range of anti-computer activities, if I may call it that, leads us to recommend a hybrid offence, namely that it may be a summary conviction offence, where the matter is not very important, or it may be an indictable offence, where lives have been lost or the economic consequences may be quite serious.

• 1615

We have embodied these suggestions in the proposed draft section, which is on page 14 of the brief.

The Chairman: Mr. Beatty, maybe you are ready to discuss some of the suggestions by Ms Kingston.

[Translation]

tion décrit l'ordinateur en fonction de ce qu'il fait plutôt que de ce qu'il est.

Deuxièmement, nous estimons qu'il faut protéger, non seulement l'ordinateur lui-même, mais aussi tous les périphériques et autres terminaux et équipements reliés à un ordinateur, sans oublier les dispositifs de télécommunication lorsqu'ils sont utilisés en conjonction avec un ordinateur. En haut de la page 9, nous proposons la définition d'un réseau informatique.

De plus, il ne suffit pas de protéger le matériel lui-même, il faut également en faire autant pour le logiciel. L'État du Michigan utilise deux définitions à cet égard, dont nous vous recommandons fortement l'examen. La première concerne un programme d'ordinateur, qui ainsi défini comme une série d'instructions ou de déclarations soumises dans une forme acceptable à l'ordinateur et qui permettent le fonctionnement d'un système informatique de façon à fournir les produits appropriés.

Voici leur définition du logiciel: un ensemble de programmes et de procédures informatiques, ainsi que les documents connexes, pour l'exploitation d'un système informatique.

Un système informatique: un ensemble de matériel informatique relié ou non à un ordinateur, et des logiciels.

M. Beatty propose de modifier l'article du Code criminel portant sur les méfaits afin d'englober toutes les infractions reliées aux ordinateurs; nous estimons que cette solution contribuerait à sous-estimer l'importance de ce genre d'infractions. Vous avez déjà entendu un grand nombre de témoignages à ce sujet et je n'ai pas l'intention d'y revenir en détail. Nous en parlons dans notre mémoire écrit.

Cependant, nous estimons que ce genre d'infraction peut être très grave et peut causer des déraillements de trains ou des écrasements d'avions, sans parler des millions de dollars qui peuvent ainsi être volés; dans certains cas, bien sûr, il ne s'agit que d'une blague d'étudiant tout à fait inoffensive, si ce n'est que des mots obscènes apparaissent sur l'écran de façon tout à fait inopportune. Toutefois, ce genre d'infraction peut être très grave même si, parfois, ce peut être simplement un méfait au vrai sens du terme. Par «méfait», on s'imagine généralement des fenêtres cassées, des salles de classes détériorées et des antennes de voitures volées. Nous estimons que les infractions reliées aux ordinateurs constituent un risque beaucoup trop grave pour les englober dans cet article.

Au chapitre des sanctions que l'on pourrait imposer dans tous ces cas d'activités anti-ordinateur, si on peut les appeler ainsi, nous recommandons la création d'une infraction hybride, c'est-à-dire qu'il y aurait déclaration sommaire de culpabilité lorsque ce n'est pas important, ou que l'on pourrait en faire une infraction criminelle lorsqu'il y a eu des victimes ou que les conséquences économiques en sont graves.

Toutes nos propositions se trouvent à la page 14 de notre mémoire.

Le président: Monsieur Beatty, êtes-vous prêt à répondre aux suggestions de M^{me} Kingston?

[Texte]

Mr. Beatty: Thank you very much, Madam Chairman. Let me first of all thank the Bar Association for their brief.

We appreciate your coming before us, and I am sure the contribution you have made today will be very helpful to us in our work, which is rapidly coming to an end.

I was not sure, Ms Kingston, in view of the fact that my bill is technically dead, whether I should resist the temptation to respond to your presentation or not. I find it irresistible.

Mr. Fortier: As we found it irresistible to comment on it.

Mr. Beatty: I appreciate that.

At the bottom of page 1:

... none of the provisions of the Bill directly face the issue raised in the case of *R. v. McLaughlin*.

In what way, if the bill were passed, could McLaughlin not have been prosecuted and convicted?

Ms Kingston: I said about use of a computer system, as opposed to a telecommunications facility.

Mr. Beatty: Where do you say that?

Ms Kingston: On page 1, fourth line from the bottom.

Mr. Beatty: About the use of a computer system as opposed to telecommunications. But the key issue here is not whether or not you can prosecute him for a telecommunication facility; but rather, whether you could prosecute him for anything.

Ms Kingston: I meant, on page 1, it did not address the issue of the use of a computer system as opposed to a telecommunications facility. That was for the point I was making.

Mr. Beatty: But nor are you suggesting, I believe, in your suggested draft section, that the issue of telecommunications facilities should be brought into that either, are you?

Ms Kingston: This is something I can perhaps better explain; but I think on page 14 of our draft, where it talks, in (2), about how everyone who without lawful excuse obtains the use of a computer system...

Mr. Beatty: Yes, but it is not a question of telecommunications. You make no attempt to tie this into the theft of telecommunications services provisions in the Criminal Code.

Ms Kingston: It is the use of a computer service. He did not necessarily call it theft of a computer service. He said, "obtains the use of a computer service".

[Traduction]

M. Beatty: Merci beaucoup, madame le président. Permettez-moi tout d'abord de remercier les représentants de l'Association du barreau canadien de nous avoir fait cet exposé.

Nous sommes heureux qu'ils aient pris la peine de se déranger aujourd'hui, et je suis sûr que leur contribution nous aidera à préparer notre rapport, dont la date approche à grands pas.

Étant donné que mon projet de loi est techniquement mort, je ne sais pas si je devrais résister à la tentation de répondre à vos remarques ou non. Toutefois, j'avoue que cette tentation est irrésistible.

M. Fortier: Et nous, nous n'avons pas pu résister non plus à faire connaître notre réaction à l'égard de ce projet de loi.

M. Beatty: Et je vous en sais gré.

Au bas de la page 1, vous dites que:

... aucune des dispositions du projet de loi ne porte directement sur la question soulevée lors de l'affaire McLaughlin.

Si le projet de loi avait été adopté, dans quelle mesure McLaughlin n'aurait-il pas pu être poursuivi et condamné?

Mme Kingston: J'ai parlé de l'utilisation d'un système d'ordinateur, par opposition à des installations de télécommunications.

M. Beatty: Où le dites-vous?

Mme Kingston: À la page 1, à la quatrième ligne en partant du bas.

M. Beatty: En effet, il est question de l'utilisation d'un système d'ordinateur par opposition à des installations de télécommunication. Toutefois, le problème fondamental ici est de savoir, non pas si l'on peut tenter des poursuites relatives à des installations de communication, mais plutôt si l'on peut tenter des poursuites en vertu d'une infraction qu'il aurait commise.

Mme Kingston: À la page 1, je ne parlais pas du problème de l'utilisation d'un système d'ordinateur par opposition à l'utilisation d'installations de télécommunications. C'était simplement pour l'argument que je défendais.

M. Beatty: Vous ne suggérez quand même pas, au chapitre de vos amendements, que les installations de télécommunications soient incluses là-dedans?

Mme Kingston: Permettez-moi de vous donner des explications. À la page 14 de notre mémoire, il est question, au paragraphe 2, de quiconque obtient, de façon illicite, l'utilisation d'un système d'ordinateur...

M. Beatty: Certes, mais il n'est pas question ici d'installations de télécommunications. Vous n'essayez pas d'inclure le vol de services de télécommunications dans le Code criminel?

Mme Kingston: Il s'agit ici de l'utilisation de services d'ordinateur, et pas forcément de vol de services d'ordinateur. En effet, le libellé stipule, «quiconque obtient l'utilisation de services d'ordinateur».

[Text]

Mr. Beatty: Yes, but there is not an attempt to tie it into the theft of telecommunications services, which was the attempt that was made to prosecute McLaughlin.

Ms Kingston: The attempt to address the issue raised in *R. v. McLaughlin* about the use of a computer system as opposed to a telecommunications facility was addressed on page 14 of our brief, (2)—“everyone who obtains the use of a computer system”. That was how we addressed it.

Mr. Beatty: In your opinion, as the bill is currently drafted, would it have been possible to secure a conviction of McLaughlin?

Ms Kingston: For the unlawful use of a computer system? No.

Mr. Beatty: No, for what took place. He accessed the computer system. He used the facilities. Ultimately some damage was done to the data base, I believe.

In particular because of the reference to the use of software in my bill, you would not dispute the fact that McLaughlin and that group had to use software?

Ms Kingston: As I discussed in my brief oral presentation, your bill would address concerns about what people might do once they accessed a computer system if they were to use unlawfully someone else's programs or someone else's data; which would address McLaughlin. However, if that person did not use someone else's data or someone else's programs, then your bill would not address the unlawful use of a computer system.

Mr. Beatty: Well, let us go, then, to the question of theft or use of computer time. I know in your oral presentation you felt it was important to include that provision, for theft of computer time. What damage is done to an institution if a computer is used, the program is not damaged in any way, the software is not damaged, and no one is deprived of the ability to use the facility?

Ms Kingston: It could be that someone is in the business because they are in a time-sharing environment, where they sell their time on a computer system and someone has used that time on their computer system.

Mr. Beatty: What would you see as an appropriate penalty for unauthorized use of computer facilities?

Ms Kingston: I think if you included computer time in the property clause, then theft of that property would probably be an appropriate offence.

Mr. Beatty: So you would define computer time as property?

Ms Kingston: That is one way you could do it, yes.

Mr. Beatty: And that is what you would recommend?

[Translation]

M. Beatty: Certes, mais n'essayez-vous pas par là d'inclure également le vol des services de télécommunications, ce qu'on avait essayé de faire en intentant des poursuites contre McLaughlin?

Mme Kingston: La question soulevée lors de l'affaire McLaughlin, et qui concerne l'utilisation d'un système d'ordinateur par opposition à l'utilisation d'installations de télécommunications, est traitée à la page 14 de notre mémoire, au paragraphe (2), où nous disons «quiconque obtient, de façon illicite, l'utilisation d'un système d'ordinateur». C'est ainsi que nous abordons le problème.

M. Beatty: À votre avis, aurait-il été possible, selon le libellé actuel du bill, d'obtenir la condamnation de McLaughlin?

Mme Kingston: Pour l'utilisation illicite d'un système d'ordinateur? Non.

M. Beatty: Non, pour l'infraction qui a été commise. Il a eu accès à un système d'ordinateur, il en a utilisé les installations et, en dernière analyse, il y a eu, je crois, détérioration de la base des données.

Plus particulièrement, étant donné que mon projet de loi fait mention de l'utilisation de logiciel, vous ne contestez pas le fait que McLaughlin et ce groupe avaient dû utiliser le logiciel?

Mme Kingston: Comme je l'ai dit tout à l'heure, votre projet de loi porte sur les actes que certaines personnes pourraient commettre une fois qu'elles ont eu accès à un système d'ordinateur, et plus précisément si elles utilisent de façon illicite les programmes ou les données appartenant à quelqu'un d'autre; cela concerne donc l'affaire McLaughlin. Cependant, si la personne en question n'a pas utilisé les données ou les programmes de quelqu'un d'autre, votre projet de loi ne règle pas le problème de l'utilisation illicite d'un système d'ordinateur.

M. Beatty: Passons maintenant à la question du vol ou de l'utilisation du temps d'ordinateur. Dans votre exposé oral, tout à l'heure, vous avez dit qu'il était important d'inclure une disposition à ce sujet. Quel tort est causé à un établissement si l'ordinateur a été utilisé, mais que le programme ou le logiciel n'a pas été détérioré et que personne n'a été privé de la possibilité d'utiliser le matériel?

Mme Kingston: Il se peut que quelqu'un veuille l'utiliser au même moment, parce qu'il partage l'ordinateur avec l'établissement en question et qu'il ne puisse pas le faire.

M. Beatty: Quelle sanction recommandez-vous en cas d'utilisation non autorisée des installations d'ordinateur?

Mme Kingston: Si vous incluez le temps d'ordinateur dans l'article sur les biens, le vol de ce bien devient alors une infraction.

M. Beatty: Vous définissez donc le temps d'ordinateur comme un bien?

Mme Kingston: C'est une façon de le définir, en effet.

M. Beatty: Et c'est ce que vous recommandez?

[Texte]

• 1620

Ms Kingston: I am saying that would be one way to do it. You were asking . . .

Mr. Beatty: Do you feel that is the preferable way, or do you feel there is another way that would be better?

Ms Kingston: I think defining "computer time" as a term might not be terrific. I might redefine it another way. But yes, I think a section dealing with the unauthorized use of computer time, computer service, however you want to define that term, would be preferable.

Mr. Beatty: Could you explain to me, technically, how—I am sure it is the case; I do not dispute it, but it would be helpful to have your guidance—you can use a computer without taking advantage of the software that is incorporated in the computer?

Ms Kingston: You may not have to take advantage of computer software. You can key on to somebody's line.

Mr. Beatty: Give me an example.

Ms Kingston: Well, I am a lawyer. I am not in the computer consulting business. I believe you did have some people before you who did discuss that issue.

Mr. Beatty: You are satisfied that it is likely, for example, in a time-sharing situation, where an individual with access to a computer—that he would be capable of doing that without using the software at all; the host computer.

Certainly I agree with you in your assessment that it is very difficult to define "computer". One of the difficulties is that anytime you begin to incorporate centres of technology in the law, you find that by the time the law is passed, it is obsolete. It is just one of the issues that we have to wrestle with on the committee.

I was struck as well by your suggestion that it could in fact include a player piano in my definition. I think that is probably a fair criticism.

First of all, you suggest that it might be useful not to define "computer", and yet in your draft section you propose defining "computer".

Ms Kingston: I said it may be useful with respect to how this bill was drafted not to include a definition of a computer.

Mr. Beatty: Do you feel that it is desirable . . .

Ms Kingston: It would depend on how a bill was drafted. If you were going to use "computer" per se as a word, then yes, you might want to include a definition in there for clarity's sake, so the public would know whether or not they were violating criminal laws.

Mr. Beatty: What element of your definition on page 14 would—is it the general purpose device section of that definition which would rule out player pianos as computers?

[Traduction]

Mme Kingston: Ce serait une façon de procéder. Vous demandiez?

M. Beatty: Pensez-vous que c'est le meilleur moyen ou estimez-vous qu'il y a une autre façon qui serait peut-être préférable?

Mme Kingston: Je pense que donner une définition du temps d'ordinateur n'est pas la meilleure solution. Pour ma part je procéderaï autrement. Mais, oui, effectivement, il serait préférable de prévoir un article sur l'utilisation frauduleuse du temps machine, du temps d'ordinateur, quelle que soit la définition de ce terme.

M. Beatty: Je suis sûr que vous avez raison mais j'ai besoin de vos lumières. Pouvez-vous m'expliquer comment on peut se servir d'un ordinateur sans se servir du logiciel qui s'y trouve?

Mme Kingston: On n'a pas besoin de se servir du logiciel. Il suffit tout simplement de se servir de la ligne de quelqu'un.

M. Beatty: Donnez-moi un exemple.

Mme Kingston: Je suis avocate. Je ne suis pas informaticienne. Je sais que vous avez entendu des témoins qui vous ont parlé de ce problème.

M. Beatty: Par exemple, dans un cas où le temps est partagé, quelqu'un pourrait se servir d'un ordinateur sans toucher au logiciel. Il suffirait qu'il ait accès à l'ordinateur, n'est-ce-pas?

Je conviens avec vous qu'il est difficile de définir le mot «ordinateur». En effet, chaque fois que l'on essaie de décrire du point de vue juridique les développements technologiques, on se rend compte, une fois la loi adoptée, que les dispositions sont déjà périmées. Ce n'est qu'un des problèmes auquel nous faisons face au Comité.

Votre allusion au piano mécanique à propos de ma définition m'a beaucoup étonné. Je pense que la critique est méritée cependant.

Vous dites, d'une part, qu'il ne serait peut-être pas utile de définir «ordinateur», mais dans l'ébauche que vous proposez, vous le faites vous-même?

Mme Kingston: J'ai dit que dans le contexte de ce projet de loi, il ne serait peut-être pas utile d'inclure une définition d'ordinateur.

M. Beatty: Pensez-vous que ce soit souhaitable?

Mme Kingston: Tout dépend de la façon dont le projet de loi sera rédigé. Si on utilisait le mot «ordinateur» seul, effectivement, il faudrait qu'il soit défini pour que le public sache à quoi s'en tenir, sache s'il commet une infraction criminelle.

M. Beatty: Je reviens à la définition que vous offrez à la page 14. Est-ce l'utilisation de l'expression «mécanisme universel» dans cette définition qui en exclut le piano mécanique?

[Text]

Mr. MacIntosh: Could you repeat that question again, please? I think the ball is in my court on that one.

Mr. Beatty: What portion of your definition of "computer" on page 14 would rule out a player piano, which Ms Kingston suggests, probably quite correctly . . .

Mr. MacIntosh: "General purpose".

Mr. Beatty: "General purpose". Is it not possible to have a computer that has a specialized purpose? And would you not then be ruling that out at the same time?

Mr. MacIntosh: The words "general purpose" have been judicially interpreted in American jurisdictions to cover this type of thing. They are used in contradiction to special purpose, where it just does one thing, to general purpose, where it does a number of things.

Mr. Beatty: Machinery that was designed, for example, to help you to regulate the use of utilities in your house; that would be a specialized-purpose machine, or a special-purpose machine, presumably.

Mr. MacIntosh: Yes.

Mr. Beatty: And yet one can easily use a computer for that, and you can have a computer that was designed expressly for that purpose. Would your definition not exclude that?

Mr. MacIntosh: The definition is intended to exclude that, and also the so-called motor vehicles which have a computer which tells when something has gone wrong with some part of the mechanism. That is a special-purpose device and is not included in this definition of "computer".

Mr. Beatty: What about computers used for air traffic control purposes and no other purpose?

Mr. MacIntosh: That is general purpose, because it does a number of things. It does not deal with just one set of data coming in; it has a number of data coming in which it deals with and gives a response on.

Mr. Beatty: A computer that is dedicated for traffic lights, for example, in the City of Ottawa: would that be general purpose or special purpose?—particularly if it were designed and built specifically for that.

• 1625

Mr. MacIntosh: We are talking about two different things here. The one that is in the little green box and goes tick, tick, tick and changes the light from red to yellow I would take to be a special-purpose one and not a computer, whereas there may be a centralized one that at 6.00 p.m. or whenever it gets dark changes the pattern to respond to traffic; and I would consider that might be a general-purpose computer.

Mr. Beatty: It may be you are making the argument strictly on the basis of case law in the U.S., and if so that is fair ball. Certainly we have no . . .

Mr. MacIntosh: I will readily concede that "computer" is an extremely difficult word to try to define and definitions

[Translation]

M. MacIntosh: Pouvez-vous répéter votre question? Je pense que c'est à moi de répondre.

M. Beatty: Quelle partie du libellé de la définition de «ordinateur» page 14, exclurait les pianos mécaniques, auxquels M^{me} Kingston a fait allusion, avec raison probablement . . .

M. MacIntosh: L'expression «universel».

M. Beatty: Je vois. N'existe-t-il pas des ordinateurs à usage spécifique? Ces derniers seraient-ils exclus?

M. MacIntosh: Le mot «universel» a été interprété par les tribunaux américains et couvre ces dispositifs. On oppose ces dispositifs universels à des dispositifs à usage spécifique, qui n'ont qu'une fonction, alors que les premiers remplissent plusieurs fonctions.

M. Beatty: Les dispositifs qui servent à régler la mise en marche des appareils ménagers seraient-ils considérés comme des dispositifs à usage spécifique?

M. MacIntosh: Oui.

M. Beatty: On peut très bien se servir de l'ordinateur dans ce cas-là, n'est-ce pas? Votre définition ne les exclurait pas?

M. MacIntosh: En effet, cette définition vise à les exclure, de même que les ordinateurs qui servent à déterminer ce qui ne va pas dans le mécanisme d'une automobile. Dans ce cas-là il s'agit de dispositifs à usage spécifique, que l'on ne veut pas englober dans la définition de «ordinateur».

M. Beatty: Et les ordinateurs dont on se sert pour l'aiguillage aérien seulement?

M. MacIntosh: Il s'agit d'ordinateurs universels, car les fonctions sont multiples. En effet diverses séries de données sont mises sur ces ordinateurs qui les traitent avant de donner une réponse.

M. Beatty: Par exemple, les ordinateurs qui servent à régler les feux de circulation à Ottawa. Dans quelle catégorie les placeriez-vous? Surtout s'ils sont conçus spécialement à cette fin.

M. MacIntosh: Nous parlons de deux choses différentes ici. Le dispositif qui se trouve dans la petite boîte verte, qui fait tic tac et permet le passage du rouge au jaune, serait considéré comme un dispositif à usage spécifique et non un ordinateur, tandis que le dispositif centralisé qui à 18 heures permet de modifier le rythme de changement des feux, en fonction de la circulation, pourrait être considéré comme un ordinateur universel.

M. Beatty: Votre argument se fonde sur la jurisprudence américaine et dans le fond, pourquoi pas. Nous n'avons certainement pas . . .

M. MacIntosh: Je reconnais que le mot «ordinateur» est très difficile à définir et que les définitions proposées qui comportent des exclusions, sont insatisfaisantes.

[Texte]

which define it and then exclude a number of things have somehow failed in what they have tried to do.

Mr. Beatty: The difficulty I have is that I want to be as broad as possible if it is necessary to legislate on computer crime. I could see untold damage being done by someone gaining unauthorized access to an air traffic control computer—or to, for that matter, even a computer that is used for traffic lights. You could find, for example, that somebody damaging the ability of the computer to function could prevent fire trucks from getting to a fire or could cause chaos in a metropolitan centre; and my concern was, essentially, if the courts were to find that a traffic computer that had as its sole function the running of the traffic lights in a city was in fact a special-purpose instrument as opposed to a general-purpose instrument that was used to balance cheque books and send electronic mail and do various and sundry other things—that we might find we had created a new loophole in the law that would not cover potential circumstances.

Mr. MacIntosh: I do not think there is a problem about that, because that type of a computer is mostly mechanical in make-up and the type of crime we are contemplating here does not happen with that type of a computer. It is a subject of attack rather than being used as an accessory to commit another crime.

Mr. Beatty: I am sorry; you have lost me there.

Mr. MacIntosh: Now we are directing ourselves to damage to the computer itself, and that is mischief. It is covered by the present Criminal Code. It is property, as the word is presently defined. That type of computer is not used, say, to steal money from a bank.

I do wish to point out that the word “computer” is used in conjunction with these other four definitions to constitute the offence and it is a bit unfair to the definition to try to single it out and criticize it because it may be inadequate as a definition of “computer” in itself.

I suggest all four definitions have to be read, and the sanction clause, in order to determine what type of computer we are talking about. Tied together, the definition of “computer”, I suggest, does become more meaningful.

Mr. Beatty: You are not dealing expressly with physical damage or physical attack upon the computer?

Mr. MacIntosh: No, we are not.

Mr. Beatty: You lost me in the distinction you were making a minute ago.

Mr. MacIntosh: No, we are not dealing with physical damage to the computer itself in this proposed section.

Mr. Beatty: That would be dealt with under the Criminal Code as things stand now, that a computer is tangible property, and if one were to get a Sir George Williams incident where a computer was damaged, that would be prosecutable today, presumably.

[Traduction]

M. Beatty: Pour ma part, je voudrais que ce soit aussi large que possible dans l'éventualité de dispositions législatives définissant des infractions relatives aux ordinateurs. On peut envisager des dégâts inouïs si quelqu'un accédait de façon frauduleuse à un ordinateur servant à l'aiguillage aérien. On peut même imaginer le pire dans le cas d'un ordinateur qui est utilisé pour les feux de circulation. On peut imaginer par exemple que quelqu'un qui causerait des dégâts à un ordinateur pourrait empêcher les voitures de pompiers de se rendre sur les lieux d'un incendie et pourrait même créer l'anarchie dans un centre métropolitain. En effet, je m'inquiète, car si les tribunaux déterminaient qu'un ordinateur servant aux feux de circulation est un dispositif à usage spécifique, plutôt qu'universel, comme c'est le cas d'un ordinateur qui sert à préparer les bilans bancaires, au courrier électronique, ou à autre chose, nous aurions créé une nouvelle échappatoire dans la loi, car toutes les situations possibles ne seraient pas envisagées.

M. MacIntosh: Je ne pense pas qu'il y ait de problème ici. En effet, ce genre d'ordinateur est surtout mécanique et le genre d'infraction auquel nous songeons ici ne met pas en cause ce genre d'ordinateur. Cet ordinateur peut subir des dégâts, mais on ne peut pas s'en servir pour commettre d'autres infractions criminelles.

M. Beatty: Excusez-moi, je ne vous ai pas suivi.

M. MacIntosh: Il s'agit ici de dégâts causés à l'ordinateur lui-même, et c'est un méfait. Les dispositions du Code criminel prévoient cela. Il s'agit de «biens», et le mot est défini. On ne peut pas se servir de ce genre d'ordinateur pour voler une banque.

Je tiens à signaler que le mot «ordinateur» est utilisé dans les quatre définitions pour décrire l'infraction, mais il ne convient pas de l'extraire de l'une d'entre elles, pour la critiquer, et lui reprocher de ne pas constituer une définition satisfaisante de l'«ordinateur».

Il faut que les quatre définitions soient lues ensemble, avec l'article portant sur la peine, afin de comprendre de quel genre d'ordinateur il s'agit. Quand on lit les quatre paragraphes ensemble, la définition de l'«ordinateur» prend toute sa signification.

M. Beatty: Vous ne parlez pas uniquement des dégâts matériels causés à un ordinateur, n'est-ce pas?

M. MacIntosh: Non, pas du tout.

M. Beatty: Je n'ai pas suivi la distinction que vous avez faite il y a un instant.

M. MacIntosh: Il ne s'agit pas des dégâts matériels que l'on peut infliger à un ordinateur.

M. Beatty: En effet, ces dégâts sont déjà prévus dans le Code criminel actuel, étant donné qu'un ordinateur est un bien et si un incident comme celui de l'Université Sir George Williams se reproduisait aujourd'hui, on pourrait tenter des poursuites, n'est-ce pas?

[Text]

Mr. MacIntosh: The hardware itself we are not dealing with, because it is presently protected; but the software, which may be lying on a table and is really part of the computer system, we are dealing with.

Mr. Beatty: Could you perhaps elaborate on the top of page 3, Ms Kingston, on computer firmware? You expressed a concern that the bill as it is currently worded might not deal with technology such as firmware. Could you elaborate for me on whether or not firmware would be patentable?

Ms Kingston: That is a very interesting issue, whether it is patentable or copyrighted or what it is. It is hard to tell whether the firmware itself is patentable, because it is encoded instructions, whether the masks that make the firmware are patentable on their own, whether each mask—or whether before you burn the masks together, you have a patent. It is very unclear. We have no cases on that in Canada.

Mr. Beatty: You expressed a concern further in the reference to making copies thereof that there might be a problem with something that is transcribed from one medium to another.

Ms Kingston: Yes.

• 1630

Mr. Beatty: How is this dealt with under the Copyright Act? If I were to tape a record, I would be transcribing it from a 45 or from an LP onto tape and would have changed the medium. My understanding is that I would be in violation of the Copyright Act, notwithstanding the fact that we had transcribed from one medium to another. Or, if you had written the lyrics for a song, and I were to sing the song, as opposed to writing it down, I would have changed the medium in which the lyrics were expressed, but presumably I would have violated copyright there too, if I had not had consent. Why would this not be a problem with the Copyright Act, but it would be a problem here if you transcribed it from one medium to another?

Ms Kingston: I took counsel from the criminal lawyers from the law firm I work at, McCarthy & McCarthy, a couple of days ago about this, and they were saying that indeed, when you prosecute in a criminal case, if the copy is in another medium, it is not a copy as far as prosecution under the Criminal Code is concerned. Why our laws are different, I have no idea. That just seems to be the state of the law today.

Mr. Beatty: On page 4 you express concern about the use of the word “divert”. Is the word not used in the Criminal Code at the present time in any section? How is it interpreted, if it is?

Ms Kingston: The problem is, I am not a criminal lawyer, I am a computer lawyer. I think when you are talking about diverting in computer systems, you would probably have to talk about changing the course. If you look at the definition of “divert” in Black’s law dictionary, as I did the other day, that is what it seems to be; that with computer technology you would be diverting or changing the course of the flow of electrons or the electronic impulses in the computer system; you would be changing its course. Its intended course was to go

[Translation]

M. MacIntosh: Il ne s’agit pas du matériel ici, car c’est déjà couvert dans le Code criminel. Le logiciel cependant, qui est quelque chose de tangible aussi, fait partie d’un système d’ordinateur, et c’est ce dont il s’agit.

M. Beatty: Madame Kingston, pourriez-vous développer ce que vous dites en haut de la page 3 au sujet du relationnel? Vous avez dit que le libellé des dispositions du projet de loi pourrait ne pas couvrir le relationnel. Sauriez-vous me dire si le relationnel peut être breveté?

Mme Kingston: C’est une question fort intéressante. Il est difficile de dire si le relationnel peut être breveté parce qu’il s’agit d’instructions encodées, et je ne sais pas si le masque de chaque relationnel peut être breveté comme tel. Je ne sais pas non plus si en les amalgamant, on pourrait demander un brevet. Ce n’est pas clair. Il n’y a pas de cas au Canada.

M. Beatty: Vous avez parlé des copies de logiciels ou de programmes d’ordinateur. Vous avez parlé du problème que pourrait causer le passage d’un support à un autre.

Mme Kingston: En effet.

M. Beatty: Comment cela est-il traité dans la Loi sur le droit d’auteur? Par exemple, si j’enregistre sur bande magnétique un 45-tours ou un long-jeu, le support a changé. Cela pourrait contrevenir à la Loi sur le droit d’auteur, même s’il y a changement de support. Autre exemple: Si vous aviez écrit les paroles d’une chanson, et si je chantais ces paroles, plutôt que de les transcrire, j’aurais changé le support, n’est-ce pas? On pourrait prétendre que je contreviens à la Loi sur le droit d’auteur également, si je n’avais pas obtenu votre permission. Dans le cas de la Loi sur le droit d’auteur, cela ne semble pas poser de problème. Pourquoi y en a-t-il un quand il s’agit de passer d’un support à un autre en informatique?

Mme Kingston: Il y a quelques jours, j’ai demandé l’avis d’avocats criminels de la firme McCarthy & McCarthy. Ils m’ont répondu que quand une copie est faite sur un autre support, et qu’on intente des poursuites criminelles, on ne peut pas invoquer les dispositions du Code criminel. Nos lois sont ainsi faites. Je ne sais pas pourquoi. Il semble que ce soit la situation aujourd’hui.

M. Beatty: À la page 4 de votre mémoire, vous soulevez la question du mot «détourner». Ce mot n’est-il pas utilisé dans le code criminel actuellement? Comment est-il interprété, éventuellement?

Mme Kingston: Je ne suis pas avocate de droit criminel, mais je suis avocate spécialisée en informatique. Quand il s’agit de détournement en matière d’ordinateur, il s’agit de changer le cours des informations. Si on se reporte à la définition du mot «détourner» dans le dictionnaire juridique Black, on constate qu’il s’agit bien de changer le cours d’une chose. Dans le cas des ordinateurs, on change le cours du flux des électrons ou des impulsions électroniques dans un système d’ordinateur. Il s’agit bien d’un changement de cours. En effet,

[Texte]

somewhere else and you are now diverting it to your own use. Even though the act of theft may, in effect, from our sort of nonlegal sense, have started in Canada when I keyed into my terminal to say that I want that information—I had thought about stealing it—I did not divert anything. Even though I keyed into my terminal, nothing happened. The information or the programs were not diverted until that went down to Buffalo and changed its course.

Mr. Beatty: I guess the ambiguity there is whether you are talking about a physical act of diversion as in diverting a water flow, or whether you are talking about... The context in which I have generally heard "diversion" used in legal terms—and I am not a lawyer—is as it relates to diversion of funds, which do not belong to you, for example. We may or may not be talking about something that was physically there; we are actually talking about something that is a little less tangible.

Ms Kingston: Yes. But the problem is in the Criminal Code. I think from our Science and Technology Committee for the Canadian Bar Association, if we were to see any changes to the law, we would feel much more comfortable if they were changes that were fairly clear and concise and were not confusing. Just on the basis of the last two minutes of our conversation, it is clear that there are possible different interpretations for the use of "divert" and it is unclear what the meaning actually is for that word. We could both argue different things. I would argue that if I typed into a terminal in Canada to say that I want information anywhere, whether it is in Ottawa or Buffalo, I have not diverted anything until I actually get that information, changing its course and coming here. Therefore I think because that definition of "divert" could be argued in court and could be listened to by judges, if we are going to have some sense out of the Clause 3 and Clause 5 recommended in this bill, it probably would be useful to couple those with a clause similar to Section 301.1(2).

Mr. Beatty: Could you just clarify this for me—and I may be a bit obtuse here. The proposed section would read as follows:

283.1 Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right diverts to his use or to the use of another person, all or part of a computer program or copy thereof or any computerized data.

Can you give me a case that would not be covered by that? What exactly do you mean?

Ms Kingston: I key into my terminal in Toronto to divert information in Buffalo. I did not commit the act in Canada. The diversion happened in Buffalo. That is why you need a clause similar to Section 301.1(2) with credit card offences: because the act of diversion did not happen in Canada.

Mr. Beatty: So the sole concern that is created is simply as it relates to international data flows.

[Traduction]

ces impulsions avaient une autre destination et vous les avez détournées à votre propre usage. Même si le vol a été initié au Canada, au moment où le terminal est mis en marche, le détournement n'a pas lieu au Canada. Même si le terminal est mis en marche au Canada, rien ne s'est encore produit. L'information ou les programmes ne sont pas détournés tant qu'ils n'ont pas quitté Buffalo.

M. Beatty: Je pense que l'ambiguïté ici vient de ce qu'il faut distinguer entre un détournement matériel, comme le cours d'une rivière, et... Je ne suis pas avocat, mais en général quand on parle de «détournement», il s'agit de détournement de fonds, d'une chose qui ne vous appartient pas. La chose n'est peut-être pas matériellement palpable. Dans le cas qui nous occupe, elle est encore moins tangible.

Mme Kingston: En effet. Le problème vient du Code criminel. Notre Comité des sciences et de la technologie, à l'Association du barreau canadien, estime que si l'on modifie la loi il faudrait que les modifications soient précises et concises et qu'elles ne prêtent pas à équivoque. À en juger d'après notre conversation depuis quelques minutes, il y a diverses interprétations possibles du mot «détourner» et on ne semble pas bien comprendre la signification du terme. Nous pourrions parler de deux choses différentes. Je pourrais prétendre que si je mets un terminal en marche au Canada et que je demande des informations ailleurs, à Ottawa ou à Buffalo, je n'ai encore rien détourné tant que je n'ai pas obtenu ces informations, tant que je n'en ai pas changé le cours. Par conséquent, étant donné la définition que l'on pourrait donner au mot «détourner» devant les tribunaux, devant les juges, il faudrait peut-être pour éclaircir les articles 3 et 5 de ce projet de loi ajouter un article semblable à l'article 301.1(2).

M. Beatty: Pourriez-vous préciser cela? Je ne sais pas si j'ai l'esprit obtus ici, mais j'ai besoin de précisions. L'article proposé dit, et je cite:

283.1 Commet un vol, quiconque prend frauduleusement et sans apparence de droit, ou détourne à son propre usage ou à l'usage d'une autre personne, frauduleusement et sans apparence de droit, tout ou partie d'un logiciel, ou copie de logiciel ou toute information mise en oeuvre sur ordinateur.

Pouvez-vous me citer un cas qui ne serait pas couvert ici? Que voulez-vous dire?

Mme Kingston: Si j'allume un terminal à Toronto pour détourner des renseignements qui se trouvent à Buffalo, l'acte n'est pas commis au Canada. Le détournement a lieu à Buffalo. Voilà pourquoi il faut adjoindre un article semblable à l'article 301.1(2) pour les cartes de crédit, car le détournement n'a pas eu lieu au Canada.

M. Beatty: L'inquiétude vient tout simplement du fait qu'il s'agit d'un flot de données qui passent une frontière, n'est-ce pas?

[Text]

• 1635

Ms Kingston: I am saying that is one of the problems we have with "divert". First of all, what does it mean, and if it does mean the actual changing of the flow of electrons where it is now coming to me instead of somebody else, so it happened outside of Canada, then due to the fact that technology today seems to expand across boundaries, then maybe to prosecute an offence we should have a section that would allow prosecution under Clause 3 and Clause 5.

Mr. Beatty: Can you think of an instance that does not involve transport or data flows where there would be a problem?

Ms Kingston: Oh, if I have tapped in from Toronto to Ottawa and did the same thing, then the whole act would have happened in Canada. If we could convince the judge that the word "divert" meant the flow of electrons, he might think it is so confusing that you cannot prosecute under the section at all; but if he was convinced that that is what "divert" meant, then the whole offence happened in Canada and you would not have to worry about that.

Mr. Beatty: Assuming that that is in fact the interpretation that he put on it, can you explain to me how it is different from what you are proposing if you gain unauthorized access to a computer? Well, it is part of one brief.

Ms Kingston: I know.

Mr. Beatty: The left hand knoweth what the right hand doeth.

Ms Kingston: I will defer to my colleague on that.

Mr. Beatty: Well, then, Mr. MacIntosh, perhaps you could then explain it to me. Assume that a computer system was located in Buffalo and I used the phone lines in Canada to access a computer system in Buffalo and American law did not, as in many jurisdictions it does not today, make it an offence for me to use the system. How would I have committed an offence in Canada simply in using the phone lines to do something in the United States that was not an offence?

Mr. MacIntosh: I do not see that an offence has happened in Canada. The bad thing has happened in the United States.

Mr. Beatty: Then it is a parallel situation to what Miss Kingston was referring to, presumably. If in fact you are dealing with a trans-border situation, the real question would be, presumably, was it an offence to do what you did in the United States that was an offence to do it in Canada? If the critical action took place in the United States, the data base was in the U.S., and if the computer that was accessed, if the services that were diverted, were in the United States,

[Translation]

Mme Kingston: Je veux dire que c'est l'un des problèmes posés par le terme «détournement». D'abord, il faudrait savoir ce que cela veut dire, et si ce terme signifie vraiment le détournement du flux électrique vers moi plutôt que vers quelqu'un d'autre, de sorte que le vol se produit à l'extérieur du Canada, il faudrait peut-être inclure quelque chose qui nous permettrait de poursuivre quelqu'un en vertu des articles 3 et 5, surtout que la technologie semble dépasser les frontières de nos jours.

M. Beatty: D'après vous, y aurait-il d'autres situations difficiles où il n'y a pas de communication de données?

Mme Kingston: Eh bien, si je parvenais, à partir de Toronto, à détourner de l'information vers Ottawa, autrement dit, si je faisais exactement la même chose, le vol aurait été commis au Canada. Il faudrait d'abord convaincre le juge que le terme «détournement» s'entend du flux électrique; il estimerait peut-être que vu la complexité de la chose, des poursuites judiciaires fondées sur cet article sont impossibles. Mais s'il était convaincu que le terme «détournement» avait cette signification précise, l'infraction aurait été commise au Canada et il n'y aurait pas de problème pour ce qui est des poursuites judiciaires.

M. Beatty: Dans l'hypothèse où il l'interpréterait ainsi, pouvez-vous m'expliquer la différence entre cela et votre proposition en cas d'accès non autorisé à un ordinateur? Vous en avez parlé dans un mémoire.

Mme Kingston: Oui, c'est exact.

M. Beatty: Cette fois-ci, la main gauche sait ce que fait la main droite.

Mme Kingston: Je demanderai à mon collègue de répondre à cette question.

M. Beatty: Monsieur MacIntosh, dans ce cas-là, vous pourriez peut-être me l'expliquer. Si je me sers des lignes téléphoniques canadiennes pour avoir accès à un système d'ordinateur situé à Buffalo et la loi américaine ne précise pas, comme c'est le cas dans bien d'autres pays, que je commets une infraction en entrant en communication avec ce système, comment pourrait-on prétendre que j'avais commis une infraction au Canada en me servant de ces lignes téléphoniques pour faire quelque chose aux États-Unis qui n'était pas considéré comme une infraction?

M. MacIntosh: À mon sens, il ne s'agirait pas d'une infraction commise au Canada. En fait, l'infraction a été commise aux États-Unis.

M. Beatty: Donc, c'est une situation semblable à celle que M^{lle} Kingston a mentionnée. S'il s'agit d'une situation où l'action a été commise dans les deux pays, je présume que l'important est de savoir si ce qui n'est pas considéré comme une infraction aux États-Unis peut l'être au Canada? Si l'action a été commise aux États-Unis, si la base de données est située aux États-Unis, et si les services d'ordinateur qui ont été détournés sont situés aux États-Unis, je présume qu'il faudrait

[Texte]

presumably you would want to look at prosecution under American law as opposed to Canadian law.

Ms Kingston: Or you might want to prosecute in Canada, in which case you may have a problem. Therefore you would need this Section 301.1 . . .

Mr. Beatty: But I think the same, presumably, would apply in this other instance, as Mr. MacIntosh was saying, that . . .

Ms Kingston: This was not intended as an entire draft bill amendment. This was just intended as a suggested draft section, not as an entire encompassing bill.

Mr. Beatty: Are you suggesting that it should be made an offence for a Canadian to access a foreign data base; that it should be an offence in Canada to gain unauthorized access to a data base in west Germany, or in Australia, or in South Africa, or in Great Britain, if it is not an offence in the host country?

Mr. MacIntosh: That is a fairly large question. I believe there are negotiations now going on in the United States as to its position with respect to this. Until every country agrees to do it, it is like protecting hijackers. Until everybody agrees that it is a bad thing and agrees to move on it at the same time, I do not think for any one country it would be wise to . . .

Mr. Beatty: I would be inclined to agree with you, and I would think that we might want to look at treaty as a way of dealing with this.

Mr. MacIntosh: But there is another matter of "divert" here, which I think "divert" might not cover, and that is where a programmer who is preparing a program plants a logic bomb in the program which is not authorized, which may or may not happen at some future time, and destroys the whole computer system upon the triggering of a message five years hence.

Mr. Beatty: How does "divert" come into that?

Mr. MacIntosh: That is what I am saying. "Divert" does not cover that type of situation.

Mr. Beatty: I do not believe that it is meant to. If we go to Clause 5 of the bill, which would amend Section 387.(1) of the Criminal Code, it would read, effectively:

387.(1) Everyone commits mischief who wilfully

(c) and without authorization, express or implied, destroys or damages a computer program or computer data or alters a computer program or computer data in a way that renders it useless or inoperative or diminishes its commercial or scientific value, . . .

It is not intended to deal with that through diversion; it is intended to deal with that through the destruction of what would then be property.

[Traduction]

examiner la possibilité d'engager des poursuites en vertu de la loi américaine, plutôt que la loi canadienne.

Mme Kingston: Il faudrait peut-être envisager de poursuivre quelqu'un au Canada, et pour l'instant, cela poserait un problème. Il faudrait que l'article 301.1 . . .

M. Beatty: Mais je crois qu'il en serait de même dans l'autre situation, comme M. MacIntosh disait, à savoir . . .

Mme Kingston: Notre intention n'était pas de proposer une modification complète du projet de loi. Nous n'avons fait que rédiger un projet d'article, qui ne couvre pas tous les aspects de la question.

M. Beatty: Proposez-vous que l'accès non autorisé à une base de données étrangère devrait être considéré comme une infraction au Canada; que l'on devrait poursuivre quelqu'un qui entre en communication non autorisée avec une base de données en Allemagne de l'Ouest, ou en Australie, ou en Afrique du Sud, ou en Grande-Bretagne, même si ce n'est pas considéré comme une infraction dans le pays où l'acte a été commis?

M. MacIntosh: C'est une question assez complexe. Je crois que des négociations sont actuellement en cours avec les États-Unis pour clarifier leur position sur cette question même. Tant que tous les pays n'auront pas accepté de le faire—c'est un peu comme les pirates de l'air. Tant que tout le monde n'aura pas reconnu que c'est un acte répréhensible qu'il faut condamner, je ne crois pas qu'un seul pays devrait prendre l'initiative . . .

M. Beatty: Je pense que vous avez probablement raison, et je crois qu'il conviendrait de régler ce problème par le biais des traités.

M. MacIntosh: Mais un autre genre de situation semblable pourrait surgir où le terme «détournement» ne s'appliquerait pas, à savoir le cas où un programmeur qui prépare un programme plante une «bombe à retardement» qui n'est pas autorisée, et qui pourrait détruire tout le système informatique si le message approprié déclenche la «bombe» à n'importe quel moment à l'avenir, peut-être dans cinq ans.

M. Beatty: Qu'est-ce que l'idée de «détournement» vient faire là-dedans?

M. MacIntosh: Justement. Le terme «détournement» ne s'applique pas à ce genre de situation.

M. Beatty: Il n'est pas censé le faire non plus. Si nous lisons l'article 5 du projet de loi, qui modifierait le paragraphe 387.(1) du Code criminel par ce qui suit:

387.(1) Commet un méfait, quiconque, volontairement,

(c) et sans autorisation, ni expresse ni tacite, endommage ou détruit un logiciel d'ordinateur ou de l'information mise sur ordinateur, ou les modifie de sorte qu'ils deviennent, l'un ou l'autre, inutiles ou inopérants ou que leur valeur commerciale ou scientifique est diminuée, . . .

Cet article aborde le problème non pas sous l'angle du détournement, mais plutôt sous l'angle de la destruction de ce qui serait considéré comme un bien.

[Text]

Mr. MacIntosh: I suggest that may not cover it either. Let us say the thing is discovered before it occurs. I would suggest there are problems in respect to a prosecution.

• 1640

Mr. Beatty: Which brings us back to Ms Kingston's portion of the brief where I believe she had referred to time bombs in programs. That is on page 5, I believe. Correct me if I am wrong, but if I understand you correctly your concern was the delayed nature of the time bomb. Could I refer you to proposed Section 387 as it stands today, which would be Sections 387.(1)(a) and 387.(1)(b):

Every one commits mischief who willfully

(a) destroys or damages property,

(b) renders property dangerous, useless, inoperative or ineffective,

If one would use a physical time bomb of some sort or arrange some sort of Rube Goldberg device which down the line was going to damage physical property, why is the principle any different there from what it would be in the case of a software time bomb?

Ms Kingston: Because I am not sure that Section 387.(1)(b) would cover that either. I am not sure what the time lag is.

Mr. Beatty: You do not think that if I were to burn your house that clearly I would have committed damage to property? There would be other provisions in the law that would apply as well, but presumably I would damage property and that might be covered there. But if I do it with an incendiary device with a timing device on it, you believe that the introduction of the timing device would render this section inoperative?

Ms Kingston: It could. Or it could because of the technology of the time bomb. The time bomb by itself may not be what actually destroys or damages something. It could be in connection with something else which only, because of the future time, is going to cause the problem, because of the nature of it. Or the internal mechanisms of a computer system could change. It can program itself, it can change itself from time to time, and it could be that you have implanted a time bomb. The time bomb by itself, if you did it at that particular time, might have rendered it useless or inoperative, but in the future it is not the time bomb by itself that does it, because of the time element, it is a combination of different things. That is why I think you run into problems with computer technology.

Mr. Beatty: It seems to me you could again draw an analogy to a physical act.

Ms Kingston: You probably could, but we were only discussing the amendments for computer crime.

Mr. Beatty: But I think I need guidance from you. I am not a lawyer myself. You are, and you have an expertise here that

[Translation]

M. MacIntosh: Mais même là, je ne crois pas que l'article s'appliquerait à ce genre de situation. Mettons que la bombe soit découverte avant d'être déclenchée. Je crois qu'il serait difficile d'engager des poursuites judiciaires.

M. Beatty: Cela nous ramène à la section du mémoire rédigé par M^{lle} Kingston où elle parle de bombes à retardement, je crois. Il me semble que c'est à la page 5. On peut me corriger, mais si je comprends bien, vous vous inquiétiez du fait que l'action de ce genre de bombes est retardée. Puis-je vous renvoyer au projet d'article 387, tel qu'il est formulé à l'heure actuelle, et plus précisément, aux alinéas (1)a) et (1)b):

«Commets un méfait, quiconque, volontairement,

(a) détruit ou détériore un bien,

(b) rend un bien dangereux, inutile, inopérant ou inefficace,»

Si on implantait une vraie bombe à retardement ou un engin du type inventé par Rube Goldberg qui détruirait un bien matériel plus tard, pourquoi le principe serait-il différent dans le cas d'une bombe à retardement implantée dans un logiciel?

Mme Kingston: Je ne suis pas sûre si on pourrait invoquer l'article 387 (1)(b) dans ce genre de situation non plus. Je ne sais pas quel décalage est prévu.

M. Beatty: Vous ne pensez pas que si je mettais le feu à votre maison, j'aurais, sans aucun doute, causé des dommages à votre propriété? Il serait peut-être possible d'invoquer d'autres dispositions de la loi, mais je présume que si je détruis ou détériore un bien, cela tomberait sous le coup de cet article. Mais d'après vous, si j'installe un mouvement d'horlogerie qui me permet de retarder le déclenchement, on ne pourrait pas invoquer les dispositions de cet article?

Mme Kingston: C'est possible. Peut-être à cause de la technologie rattachée à la bombe à retardement. Il est possible que ce ne soit pas la bombe elle-même qui détruit ou détériore un bien. La cause pourrait être quelque chose qui ne se produira qu'à l'avenir, étant donné la nature de l'engin. Ou bien le fonctionnement interne du système informatique pourrait changer. Il peut établir ses propres programmes, il peut les changer de temps en temps. Si une bombe à retardement a été implantée, la bombe elle-même, si elle est déclenchée à un moment donné, pourrait détruire le système ou le rendre inutile ou inopérant; mais si nous parlons de l'avenir, ce n'est pas la bombe à retardement elle-même qui en est responsable, étant donné le décalage. En fait, c'est une combinaison de facteurs. Voilà pourquoi je pense que la technologie informatique pose un problème.

M. Beatty: Mais encore une fois, il me semble qu'on pourrait appliquer le principe par analogie avec l'acte matériel.

Mme Kingston: C'est fort possible, mais nous parlons uniquement des modifications à faire en ce qui concerne les infractions relatives aux ordinateurs.

M. Beatty: J'ai besoin de vos conseils. Je ne suis pas avocat. Étant donné que vous l'êtes, vous avez des connaissances que

[Texte]

I do not have. The question that came to my mind is, it is easier for me to argue from an analogy and if this section be applicable in delayed damage to property as it relates to (a) and (b), why would not the new (c) be applicable also? Or, if (a) and (b) would not be applicable, if there is an element of time involved there, why would that be the case? I just do not understand it as a non-lawyer.

Ms Kingston: Unfortunately, I am not a criminal lawyer. As you know, lawyers tend to specialize these days and I am in a law firm where we all specialize.

Mr. Beatty: But you believe there would be a differentiation between the destruction of tangible property and the destruction of software?

Ms Kingston: No, I think there could be a differentiation between computer technology, because I think computer technology has the ability to program itself and to change itself. That is where I think the time element becomes more critical with computer technology than it may with something else.

Mr. Fortier: If I may intervene, I am not a computer specialist but I have done some criminal work and I also am still labelled as a generalist on occasion. Even addressing the non-computer technology and the example which you are discussing at the moment, if the damage is prevented, let us say it is not a computer-related device, I do not know if that is even conceivable, but if the damage is not caused when the device is uncovered I do not think the mischief section would adequately deal with it.

Mr. Beatty: Yes, and the same would apply with regard to physical damage to real property. If I had arranged some device that would damage this chair tomorrow afternoon and you caught it now, presumably these sections of the code would not apply there.

Mr. Fortier: Would not apply, that is correct.

Mr. Beatty: Yes. I think it is a fair criticism you make that the planting of such a device might be something you would want to cover, as well as the actual use of it.

Mr. Fortier: Yes.

Mr. Beatty: Just one final point with regard to Ms Kingston's presentation. I am sorry we do not have a transcript as yet, but I believe in your oral testimony you made reference to the destruction of programs or data that may not be covered by this destruction...

• 1645

Ms Kingston: I think I was referring to the values. It was defined in Clause 5 of the bill, relating to proposed Section 387.(1)(c) of the act, which refers to computer programs or computer data. It makes a distinction from the definition in Clause 4 of the bill which talks about computer software programs and not just computer programs. Also, it talks about

[Traduction]

moi, je n'ai pas. La question qui me vient à l'esprit est la suivante: Est-il plus facile de raisonner par analogie et, de plus, si l'article en question peut être invoqué lorsqu'il y a détérioration différée d'un bien selon les termes des alinéas a) et b), l'alinéa c) ne pourrait-il pas être invoqué également? Comme je ne suis pas avocat, je ne comprends pas très bien tout cela.

Mme Kingston: Malheureusement, je ne suis pas criminaliste. Comme vous le savez, les avocats ont tendance à se spécialiser de nos jours et je fais partie d'un cabinet d'avocats où tout le monde est spécialisé.

M. Beatty: Mais pensez-vous qu'il y a une différence entre la destruction d'un bien tangible et la destruction d'un logiciel?

Mme Kingston: Non, mais je pense que la situation pourrait être quelque peu différente lorsqu'il est question de technologie informatique du fait que les ordinateurs peuvent établir leurs propres programmes et les changer. C'est là que l'aspect de décalage est plus important qu'il ne le serait dans une autre situation.

M. Fortier: Si vous me permettez, je ne suis pas un spécialiste du domaine des ordinateurs mais j'ai eu l'occasion d'étudier le droit pénal et de temps en temps, on m'appelle même un généraliste. En ce qui concerne la technologie non rattachée à l'ordinateur et l'exemple dont vous êtes en train de discuter, si l'on parvient à éviter que les dommages ne soient causés—supposons qu'il ne s'agisse pas d'un engin informatique; en fait, je ne sais même pas si c'est possible—mais si les dommages n'ont pas été causés au moment où l'on découvre l'engin, je ne crois pas qu'on pourrait invoquer l'article sur le méfait.

M. Beatty: Oui, et il en serait de même dans le cas de dommages matériels causés à un bien tangible. Si j'implantais un engin dans cette chaise qui causerait sa destruction demain après-midi et que vous le découvriez aujourd'hui, il est normal que ces articles du Code ne s'appliquent pas.

M. Fortier: Oui, ils ne s'appliqueraient pas.

M. Beatty: Oui. Je crois que vous avez raison de dire qu'il faudrait prévoir l'implantation et l'utilisation effective de ce genre d'engin dans le Code.

M. Fortier: Oui, c'est vrai.

M. Beatty: J'ai un dernier point à soulever au sujet de l'exposé de M^{lle} Kingston. Malheureusement nous n'avons pas encore reçu les procès-verbaux, mais je crois que dans votre témoignage, vous avez fait allusion à une situation où la destruction d'un certain type de logiciel ou d'information ne serait pas prévue...

Mme Kingston: Je pense que je parlais de la valeur. La définition qui figure à l'article 5 du projet de loi, qui prévoit le projet d'alinéa 387(1)(c) de la Loi, et qui porte sur les logiciels d'ordinateur ou l'information mise sur ordinateur. Elle est différente de la définition qui figure à l'article 4 du projet de loi, dans laquelle on parle de logiciel d'ordinateur, et pas

[Text]

retrievable computer data or information, and not just computer data as referred to in Clause 5. That is why I did not understand the difference.

Mr. Beatty: I believe at the time you mentioned it though, it was in the final section at the bottom of page 5, where you are dealing with:

“diminishes its commercial or scientific value”

Ms Kingston: I am sorry. I was talking about the commercial or scientific value.

Mr. Beatty: I think it may just have been a slip where you refer to the destruction of software. It would seem to me that section, as it is proposed here, would certainly cover the destruction of software in that it says: “. . . renders it useless or inoperative . . .” —and destruction would surely apply. You would not have to establish any commercial value or scientific value. If it is destroyed, it is destroyed.

Ms Kingston: Well, it may not be useless or inoperative.

Mr. Beatty: How can you destroy something without making it useless or inoperative? If I were to destroy your car, I would suspect that probably would mean that I have made it useless and inoperative.

Ms Kingston: What happens if you just destroy part of it?

Mr. Beatty: Then I have destroyed part of your car.

Ms Kingston: Or if you alter it?

Mr. Beatty: Then I have not destroyed it.

Ms Kingston: That is right.

Mr. Beatty: But you used the word “destruction” yourself. It was the use of the word you had that I was querying.

Mr. Kingston: I am sorry. In the hurry of making my oral testimony, I should have said, “destroy, damage or alter”.

Mr. Beatty: I will depart from Mitel for the time being because my own thoughts have evolved considerably as a result of the testimony we have had. Probably, Mr. MacIntosh, you would be the appropriate person to ask, and I wonder if you feel that it would be better to deal with the issue of computer abuse through a computer statute, as such. Or would it be better for this committee to recommend that what we should be doing is to deal with it in nibbles in different places? For example, I wonder whether there should be an amendment to the Copyright Act separately to deal with the question of computer software and programs.

Second; perhaps it might be useful to create an offence of computer trespass or unauthorized access, which I think is similar to many of the concerns which were suggested, to close off that loophole of unauthorized access which, as Miss Kingston, properly pointed out, is not dealt with in my bill. It

[Translation]

seulement de programmes d'ordinateur. De plus, on parle de toute information entrée sous une forme repérable par ordinateur, et pas simplement d'informations mises sur ordinateur, comme à l'article 5. Alors, je ne comprends pas très bien la différence entre les deux.

M. Beatty: Au moment où vous l'avez mentionné, toutefois, je pense que vous faisiez allusion au dernier article, au las de la page 5, où l'on lit:

« . . . ou que leur valeur commerciale ou scientifique est diminuée ».

Mme Kingston: Je suis désolée. En effet, je parlais de la valeur commerciale ou scientifique.

M. Beatty: Je pense que votre référence à la destruction de logiciel est simplement une erreur. Il me semble que ce projet d'article, tel qu'il est rédigé ici, prévoit sans aucun doute la destruction de logiciel, car il dit bien « . . . rend un bien inutile ou inopérant . . . »; donc, il s'agirait sûrement de destruction. Il ne serait pas nécessaire d'établir sa valeur commerciale ou scientifique. Si un bien est détruit, il est détruit.

Mme Kingston: Eh bien, il ne serait pas forcément inutile ou inopérant.

M. Beatty: Comment peut-on détruire quelque chose sans le rendre inutile ou inopérant? Si je détruisais votre voiture, je présume que je la rendrais inutile et inopérante.

Mme Kingston: Et si vous n'en détruisiez qu'une partie?

M. Beatty: J'aurais tout de même détruit une partie de votre voiture.

Mme Kingston: Et si vous la modifiez?

M. Beatty: Dans ce cas-là, je ne l'aurais pas détruite.

Mme Kingston: C'est exact.

M. Beatty: Mais vous-même avez parlé de « destruction ». C'est votre choix de ce mot en particulier que je ne comprenais pas.

Mme Kingston: Je suis désolée. Je pense que j'étais un peu pressée lors de mon témoignage; j'aurais dû dire: « détruit, détériore ou modifie ».

M. Beatty: Je laisserai tomber la question de Mitel pour l'instant car mes idées ont beaucoup évolué par suite des témoignages que nous avons reçus. Monsieur MacIntosh, vous êtes sans doute le mieux placé pour répondre à cette question: Estimez-vous qu'il vaudrait mieux s'attaquer au problème des délits informatiques par le biais d'une loi spécifique sur les ordinateurs? Ou ce Comité devrait-il recommander que nous nous attaquions au problème en modifiant plusieurs lois? Par exemple, je me demande si l'on devrait modifier la Loi sur le droit d'auteur pour traiter de la question du logiciel et des programmes d'ordinateur.

Deuxièmement, il serait peut-être utile de préciser dans la loi que l'accès non autorisé à un ordinateur est une infraction, ce qui serait semblable à nombre des propositions qui nous ont été faites pour éliminer cet échappatoire de l'accès non autorisé qui, comme M^{lle} Kingston l'a signalé, n'est pas

[Texte]

would still be legal to access a computer if you did not do any damage when you were there.

Third, we might want to recommend that studies be done on provisions of trade secrets legislation.

Fourth, at a later date we might want to take a look at a data security standards for institutions which hold information about third parties. For example, if you had my credit records or my medical records, you would be required to maintain them in a way that protected them from unauthorized access.

How should we deal with all this? Should there be one computer bill trying to deal with computer issues, or should we recommend that we try to deal with offences relating to computer use from the point of view of what the effect is, or what the property is which, in fact, is involved—whether it be computerized or whether it be manually held?

Mr. MacIntosh: My reaction is both. There is a valid argument that there should be a criminal offence with respect to the altering of data and so on or stealing computer time in a big way, where it has a serious economic effect or an effect upon somebody's livelihood.

But the other matters you mentioned are all areas where there is a great lack of control at the present time. The present laws do not appear to be adequate to cover most of the areas you have mentioned. Now a bill of this magnitude would take several years in the doing, I would suggest, whereas on the criminal sanction, it is fairly obvious what should be done. We may be arguing back and forth about the appropriate wording but I think the basic intent is much the same.

Mr. Beatty: We attempt to protect software, though, from the point of view of copying. I notice that you do not refer to the copying of software in your draft clause, which, on the other hand, I did. I assume from that omission that it would be your feeling it would be better dealt with in revisions to the Copyright Act rather than in a computer bill per se.

Mr. MacIntosh: No, our act does protect software because it protects the computer system, and computer system has an extended definition to include computer software. So we are concerned about the software lying on the table.

Mr. Beatty: But even if you stored a computer program on a magnetic cassette and I just borrowed the cassette, put it in my tape recorder and down-loaded the program into my computer, I would have committed an offence under your bill.

Mr. MacIntosh: That is right, because the owner of the program has the right to the exclusive use of that program.

[Traduction]

envisagée dans mon projet de loi. Il serait toujours légal d'avoir accès à un ordinateur si on ne causait pas de dommage.

Troisièmement, nous devrions peut-être recommander que des études se fassent sur les dispositions de la loi portant sur les secrets commerciaux.

Quatrièmement, à une date ultérieure, il faudrait peut-être examiner la possibilité de créer une norme de sécurité applicable aux établissements qui possèdent des renseignements sur des tiers. Par exemple, si vous possédiez un dossier sur ma solvabilité, ou encore mon dossier médical, vous seriez tenu de les protéger contre l'accès non autorisé.

Donc, comment devons-nous aborder tous ces problèmes? Faudrait-il avoir une seule loi pour traiter de toutes ces questions informatiques, ou devrions-nous recommander plutôt que chaque infraction soit abordée individuellement du point de vue de l'effet de l'acte commis ou du genre de bien dont il s'agit—qu'il s'agisse d'informations mises sur ordinateur ou d'un appareil qu'on peut tenir à la main?

Mr. MacIntosh: Je pense qu'il faut faire les deux. Une façon tout à fait valable d'aborder la question serait de créer une infraction pénale en cas de modification de données informatiques ou de vol de temps de machine, lorsqu'ils ont une grave incidence économique sur la capacité d'une personne de gagner sa vie.

Mais les autres domaines que vous avez mentionnés manquent tout à fait de contrôle à l'heure actuelle. Les lois actuelles ne semblent pas être suffisantes pour prévoir la plupart des situations que vous avez mentionnées. Il faudrait plusieurs années, sans doute, pour rédiger un projet de loi d'une telle portée alors que du côté du droit pénal, la voie à suivre est plus ou moins évidente. On pourrait toujours contester le libellé, mais je crois que l'intention fondamentale reste la même.

Mr. Beatty: Toutefois, il faut essayer de protéger le logiciel contre la reproduction non autorisée. J'ai remarqué que vous ne mentionnez pas la reproduction non autorisée de logiciel dans votre projet d'article comme je l'ai fait dans mon projet de loi. Si vous l'avez omis, je présume que vous estimez qu'il vaudrait mieux aborder cette question en modifiant la Loi sur le droit d'auteur plutôt que de l'inclure dans une loi sur les ordinateurs.

Mr. MacIntosh: Non, en fait, notre loi protège le logiciel en accordant une protection au système informatique et notre définition de système informatique est suffisamment générale pour comprendre le logiciel. Par contre, ce qui nous intéresse, c'est le logiciel qu'on trouverait sur une table, par exemple.

Mr. Beatty: Mettons que vous avez emmagasiné un programme d'ordinateur sur une cassette magnétique; si j'empruntais cette cassette et que j'introduise votre programme dans mon ordinateur, j'aurais tout de même commis une infraction au regard de votre projet de loi.

Mr. MacIntosh: C'est exact, car le propriétaire du programme est le seul qui ait le droit de l'utiliser.

[Text]

Mr. Beatty: Why do you feel that should not be dealt with in the context of copyright as opposed to being dealt with in a computer bill per se? I am inclining away from the direction I propose in my bill—just the opposite one—whereby I felt that it might be better to revise the Copyright Act and treat computer programs the same way you would lyrics to a song or a manual for working a DC-10. These are, in essence, instructions to program machinery to get a certain response from it, and you should try to deal with them in as broad a way as possible without trying to treat computerized information in a way different from other information.

Mr. MacIntosh: Well, I see this as a matter of degree. It is one thing to steal cooking recipes off my home computer but it is another thing to penetrate a government computer and come up with a list of the agents of a foreign nation who have been uncovered.

Mr. Beatty: But in terms of software, presumably that would not be part of the software. If it is a set of operating instructions, would it be of more concern to you if it relates to a computer than if it relates to another device, from the point of view of copyright?

Mr. MacIntosh: Copyright basically leads to a civil remedy. In other words, you sue them and get money damages. And there are circumstances where that is just not appropriate, where in effect there has been a blatant theft of something and where somebody is using something which is not his.

Mr. Beatty: I will wrap up very shortly, Madam Chairman. You have been very patient, as has my colleague Mr. Robinson.

One of the things I have been trying to avoid, as a result of the testimony we have had, is doing what I did in my bill, and that is to treat information as property, except in the most extraordinary circumstances. We do accept that there is intellectual property, as relates to copyright, and so on, and if copyright will cover it, that is great.

My concern is that you create a disequilibrium in the law if you say that information stored in a computerized form will be treated differently by the police than will unauthorized access to information stored in your briefcase. Why should the form of storage of information be more important than the nature of the information itself? Is it advisable for us to create . . . ? In order to close off the loophole you have today, where it is quite possible for me to access your computer without committing an offence, whereas if I were to break into your office and steal a file, or even copy a file that was in your office, I would be guilty of break and enter, trespass and possibly theft—in order to close off the imbalance, there is one way. Why should we create new disequilibriums in the law, based on the nature of storage of information rather than the nature of the information itself?

[Translation]

M. Beatty: Pourquoi pensez-vous qu'on ne devrait pas aborder cette question dans le contexte du droit de l'auteur, mais plutôt dans une loi spécifique sur les ordinateurs? J'ai maintenant tendance à préconiser une autre méthode d'approche que celle que j'ai adoptée dans mon projet de loi—en fait, l'approche contraire—alors qu'au départ j'estimais qu'il serait peut-être préférable de modifier Loi sur le droit d'auteur et de traiter des programmes d'ordinateur de la même façon que les paroles d'une chanson ou le manuel d'instructions d'un avion DC-10. Il s'agit, essentiellement, d'instructions qui vous permettent de faire fonctionner une machine de façon à obtenir une réponse, et il faudrait essayer d'adopter une approche générale sans vouloir traiter de l'information mise sur ordinateur différemment de toute autre information.

M. MacIntosh: Eh bien, à mon sens, c'est une question de degré. C'est une chose que de voler les recettes de cuisine que j'ai emmagasinées dans mon ordinateur à la maison, mais cela en est une autre que d'avoir accès à un ordinateur gouvernemental et d'obtenir une liste de tous les agents d'une nation étrangère qui ont été démasqués.

M. Beatty: Mais on peut présumer que ces instructions ne feraient pas partie du logiciel. Si nous parlons d'un ensemble d'instructions, est-ce que le problème est plus grave dans le cas de l'ordinateur que dans le cas d'un autre genre d'appareil, du point de vue du droit d'auteur?

M. MacIntosh: Le droit d'auteur permet de régler le problème par le biais du droit civil. Autrement dit, vous poursuivez quelqu'un et on vous accorde de l'argent à titre de dédommagement. Or, dans certaines situations, ce n'est pas possible; par exemple, lorsque quelque chose a été manifestement volé et que quelqu'un utilise quelque chose qui n'est pas à lui.

M. Beatty: Je vais bientôt terminer, madame le président. Vous avez été très patiente, tout comme mon collègue M. Robinson.

Ce que j'essaie d'éviter, après avoir entendu certains témoignages, est justement ce que j'ai fait dans mon projet de loi, à savoir de considérer l'information comme un bien, sauf dans des situations exceptionnelles. Nous acceptons le concept d'un bien intellectuel, dans le domaine du droit d'auteur, et si on peut l'aborder dans le contexte de la Loi sur le droit d'auteur, ce serait très bien.

Mais je m'inquiète du déséquilibre qu'on créerait dans la loi si on prévoit que l'information mise sur ordinateur sera traitée par la police différemment de l'information contenue dans votre serviette qu'on obtiendrait sans permission. Pourquoi la forme d'emmagasinage ou le support, serait-il plus important que la nature de l'information elle-même? Convient-il de créer . . . Pour éliminer l'échappatoire qui existe actuellement, et qui me permet d'avoir accès à votre ordinateur sans que cela soit considéré comme une infraction, alors que si j'entre par effraction dans votre bureau et j'y vole un dossier, ou même si je reproduis un dossier que vous avez dans votre bureau, je serai coupable d'effraction, d'intrusion et peut-être de vol—donc, il y a un moyen d'éliminer ce déséquilibre. Pourquoi créerions-nous un nouveau déséquilibre dans la loi, en prenant

[Texte]

Mr. MacIntosh: I would suggest that the reason is the nature of the offence to get that stored information; generally a very sophisticated approach has to be made to enter the computer, and in the process other information may be damaged.

Mr. Beatty: What if I damaged information that was in your filing cabinet? Say it was trade secrets we were concerned about. If you had a large company, say it was an oil company, and you were storing records having to deal with test drilling in particular areas, or geological surveys where you felt there was a new area which might be very promising, and I was working for a competitor, gained access to your computer and was able to get information from you which would enable me to gain competitive advantage. Why does it greatly make any difference whether I gained it from your computer or from your filing cabinet? Is it not the nature of the information as opposed to the nature of the storage that is important?

• 1655

Mr. MacIntosh: Of course, that is a valid argument. About all I can say is, to repeat myself, it is the manner required in the penetration of the security of the system to get the information that makes it a more heinous offence to get it out of the computer than out of the filing drawer.

Ms Kingston: I think it is also a matter of addressing the needs of society, which do change from time to time. I think one of the needs of society, whether justified or not, is the fact that if they have something in the vault then someone has to go to great lengths to get there. They have to break into the house; they have to go to that source. Whereas if it is in a computer system, someone down in California can get it and they do not even know about it. I think that is a concern of society which has been raised.

Those rumours I was talking about in my oral presentation, and something to be addressed in your bill, is that society is concerned with information in computerized form, or machine readable form, and they have lost control of it. Because of the use of computers being so wide-spread in our society, at this stage one almost has to be computerized to keep up with competition, and that is why they are so concerned about the lack of control. They feel they do not have the same lack of control with a vault, because it is right there in their office or right wherever it happens to be. But with computerized information they do not know who has it.

Mr. Beatty: It could be a delusion.

Ms Kingston: It could be. But real or not, that is perceived as society's needs.

Mr. Beatty: In the case of my office, I feel that the information stored in my Micom and disettes is safer than the information stored manually in my filing cabinets, because anybody who knows how to read English can understand what is going into my filing cabinets.

[Traduction]

comme point de repère la façon dont cette information est emmagasinée plutôt que la nature de l'information elle-même?

M. MacIntosh: Je pense que c'est à cause de la nature de l'infraction commise en essayant d'obtenir cette information; généralement, il faut être très habile pour entrer en communication avec un ordinateur, et il est possible que les informations soient endommagées en même temps.

M. Beatty: Et si j'endommageais de l'information contenue dans votre classeur? Supposons qu'il s'agisse de secrets commerciaux? Si vous étiez le directeur d'une grande compagnie, disons une compagnie pétrolière, et que vous conserviez des dossiers sur les tests de forage dans diverses régions ou des levés géologiques concernant de nouvelles régions prometteuses, et si moi, qui travaillais pour un concurrent, je réussissais à avoir accès à votre ordinateur et à obtenir des renseignements qui me permettraient de prendre le dessus, peu importe que je prenne ces renseignements de votre ordinateur ou de votre classeur, n'est-ce pas? N'est-il pas vrai que la nature de l'information est plus importante que le lieu ou la nature de l'emmagasinement?

M. MacIntosh: Bien sûr, c'est un argument valable. Tout ce que je peux vous dire, au risque de me répéter, c'est que le mode d'intrusion dans le système d'ordinateur pour obtenir ces informations rend l'infraction plus grave que si vous cherchiez à obtenir ces renseignements dans un simple classeur.

Mme Kingston: Il s'agit également de répondre aux besoins de la société, besoins qui évoluent. L'un de ces besoins, qu'il soit justifié ou non, c'est que lorsque ces renseignements sont gardés dans un coffre-fort, il faut se donner beaucoup de peine pour aller les y chercher. Par contre, si ces informations sont emmagasinées dans un ordinateur, une personne se trouvant en Californie peut y avoir accès à l'insu de leur propriétaire. C'est donc un problème pour la société.

Je parlais également tout à l'heure de l'inquiétude que nourrit apparemment l'opinion publique à l'égard des renseignements informatisés, qui échappent donc à son contrôle. Étant donné l'utilisation grandissante des ordinateurs, chaque entreprise est pratiquement obligée d'avoir son ordinateur afin de faire face à la concurrence, et c'est la raison pour laquelle le public s'inquiète du manque de contrôle qu'il peut exercer à l'égard des renseignements qu'ils contiennent. Il estime en effet qu'il ne peut pas exercer le même contrôle qu'à l'égard d'un coffre-fort, qui se trouve bien et bien au bureau ou dans un autre local. Avec les renseignements informatisés, nul ne sait qui peut y avoir accès.

M. Beatty: C'est peut-être une simple illusion.

Mme Kingston: Peut-être, mais qu'elle soit réelle ou non, c'est une inquiétude de la société en général.

M. Beatty: En ce qui me concerne, j'estime que les informations emmagasinées dans mon Micom et dans ses disquettes sont bien plus à l'abri que les informations que j'ai moi-même placées dans mes tiroirs, car quiconque comprend l'anglais

[Text]

Ms Kingston: But presumably the law is to meet the needs of society, and I think that is the need of society.

Mr. Beatty: But real needs as opposed to perceived needs, presumably. I do not argue this point . . .

Ms Kingston: I think it is a real need. I think your first question was more valid: should that need be addressed by criminal sanctions or not? I think it really is a real need. I mean, technology has advanced to a very large state, where that really is a real need—that you have lost control of it.

Mr. Beatty: Yes, I agree. And that is just why I said that unauthorized access or data trespass, computer trespass, might be one way of dealing with that.

Ms Kingston: But your question to Mr. MacIntosh, as to whether or not that should be addressed by five separate bills or whatever—you know, your copyright bill—or be addressed by criminal law, I do not think that question is that valid. I think whether it is addressed by criminal sanctions or not is a completely different question from whether or not it should be addressed in the Copyright Act or whether it should be left to common law or should there be a trade secret common law statute enacted. Those are all separate concerns.

If you are addressing it civilly, the question is, how do we address it? But it is not a question of do we address it civilly or criminally; I think it is both.

Mr. Beatty: We could do both. Thank you very much for a very, very helpful presentation from all of you. I appreciate it very much. Thank you, Madam Chairman, for your patience.

The Chairman: Thank you. Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Thank you, Madam Chairman. At the outset I want to thank the members of the Canadian Bar Association for appearing before us today. As a member of the Canadian Bar Association myself, I always appreciate their quickness in responding to the needs in the House of Commons and coming to give us the benefit of their wisdom and expertise. So once again I can just welcome them. I have met with them so many times over the years, and it is just another occasion when we can take advantage of their good nature and their high quality of discussion and contribution.

At the outset I would like to suggest, Madam Chairman, that the brief be incorporated in our minutes because it has been referred to but it has not been read into the record; that is, all of it has not been read into the record. There are some parts which I think are very important but have been sort of brushed over or almost overlooked. So I would suggest that be done.

The Chairman: D'accord.

[Translation]

peut prendre connaissance de ce qui se trouve dans mes classeurs.

Mme Kingston: Toutefois, la loi se doit de répondre aux besoins de la société, et c'en est un à mon avis.

M. Beatty: Il s'agit cependant de faire la différence entre les besoins réels et les besoins perçus. Je ne conteste pas votre argument . . .

Mme Kingston: Je pense qu'il s'agit d'un besoin réel. Toutefois, votre première question était plus valable, puisque vous demandiez si ce besoin devrait être satisfait par des sanctions pénales ou non? À mon avis, il s'agit d'un besoin réel. La technologie a pris une importance extrêmement grande et, étant donné que vous en avez perdu le contrôle, il s'agit bien d'un besoin réel.

M. Beatty: J'en conviens, et c'est justement la raison pour laquelle je pensais, dans mon projet de loi, qu'en parlant d'accès illicite ou d'intrusion dans les données ou dans les ordinateurs, ce serait une façon de régler le problème.

Mme Kingston: Toutefois, lorsque vous demandez à M. MacIntosh si la façon de procéder consistait à modifier cinq bills différents, notamment le bill sur le droit d'auteur, ou bien s'il fallait modifier le droit pénal, je ne pense pas que ce soit une question valable. Que ce problème soit réglé par des sanctions pénales ou non, c'est tout à fait différent que de se demander s'il devrait être réglé par la Loi sur le droit d'auteur ou par la *common law*, ou encore par une loi de *common law* sur les secrets commerciaux. Tous ces problèmes sont différents.

Si vous voulez le régler par le droit civil, la question est de savoir comment procéder. Toutefois, il ne faut pas se demander si ce problème doit être réglé par le droit civil ou par le droit pénal, car il faut les deux à la fois, à mon avis.

M. Beatty: C'est possible. Merci beaucoup de nous avoir donné autant de renseignements utiles. Merci beaucoup, madame le président, d'avoir été si patiente.

Le président: Merci. Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Merci, madame le président. J'aimerais d'emblée remercier les membres de l'Association du Barreau canadien de comparaître devant nous cet après-midi. En tant que membre de cette association moi-même, j'ai toujours apprécié sa diligence à répondre aux invitations de la Chambre des communes de venir partager avec nous son expérience. Je souhaite donc la bienvenue à ses représentants. Je les ai rencontrés tellement souvent au cours des dernières années, que c'est simplement une occasion de plus, pour moi, de participer à une discussion aussi intéressante.

J'aimerais tout d'abord proposer, madame le président, que le mémoire soit annexé à notre compte rendu car, bien qu'il ait été présenté, il n'a pas été consigné au compte rendu, tout au moins dans son intégralité. Certaines parties sont très importantes et ont jusqu'à présent été survolées ou pratiquement négligées. J'aimerais donc proposer que ce document soit annexé.

Le président: Agreed.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): You know, Miss Kingston, what you have really done is virtually destroy the bill in its entirety. It makes me think of *Alice in Wonderland* and that little ditty about Humpty Dumpty:

Humpty Dumpty sat on a wall, Humpty Dumpty had a great fall,
All the King's horses and all the King's men
Couldn't pick Humpty Dumpty up again.

Mr. Beatty: That was "Could not put Humpty Dumpty together again" I think.

Mr. Robinson (Etobicoke—Lakeshore): Well, put him up again or put him together again.

It seems to me that maybe you could have done us a favour by not only destroying the bill but also trying to build on the thought or the idea there, try to reconstruct it in some way and present it to us that way.

• 1700

But you have chosen instead to come up with a suggested draft section of the Criminal Code provisions. I do not want to go into the questioning that my colleague had as to whether you prefer the Criminal Code approach or to go into some other approaches. I noticed when he mentioned the Copyright Act and Patent Act and certain others there was a nodding of heads, but there was no verbalizing of what suggestions for change you might be prepared to make or whether you had even considered this.

Maybe I should let that be my first question. Have you really considered any changes in any other statutes, other than the Criminal Code; and to what extent?

Ms Kingston: I would love to see the Copyright Act changed. We could talk for hours on that. I spend a lot of time on that act.

I think a lot of constructive help could be made if the Copyright Act were amended to take into account this technology.

Mr. Fortier: I think I can answer your question also by repeating, Madam Chairman, what I said earlier. This report, this submission, has come directly to you from Law, Science, and Technology without having followed the usual channels of CBA briefs. The usual channels include a dissemination of such a brief to all our sections and all our committees for their comments and input. But this would have taken too long, and we thought you wanted to hear us, so we decided we were going to come now and do the remainder later. So we will have in due course reactions from committees such as the Patent, Trademark and Copyright Committee. But it has not been done yet, sir.

Mr. Robinson (Etobicoke—Lakeshore): I noted that the presentation was being made by a lawyer who has avowed on several occasions that she is a computer lawyer and not a criminal lawyer. Yet most of the brief seems to be criminal in nature.

Ms Kingston: It is a computer-related nature.

[Traduction]

M. Robinson (Etobicoke—Lakeshore): En fait, madame Kingston, vous avez pratiquement détruit le bill dans sa totalité. Cela me rappelle Alice au pays des merveilles et cette fable de Perrette et le pot au lait:

Adieu veaux, vaches, cochons, . . .

M. Beatty: C'est bien cela.

M. Robinson (Etobicoke—Lakeshore): Essayons donc de récupérer les pots cassés!

A mon avis, vous auriez pu, après avoir démolì le bill, essayer au moins de nous en proposer un autre.

Mais vous avez plutôt choisi de proposer des amendements à certaines dispositions du Code criminel. Je ne voudrais pas remettre en question ce qu'a dit mon collègue quant à savoir si vous préférez attaquer ce sujet en vous servant du Code criminel ou autrement. Quand il a parlé de la Loi sur le droit d'auteur ou de la Loi sur les brevets et de certaines autres, je me suis aperçu qu'il y en a plusieurs qui hochaient la tête, mais personne ne s'est aventuré à faire de propositions concrètes ou n'a même dit que vous aviez étudié ces possibilités.

Peut-être devrait-ce être là ma première question. Avez-vous sérieusement songé à modifier d'autres lois, c'est-à-dire autres que le Code criminel et jusqu'à quel point?

Mme Kingston: J'aimerais bien voir changer la Loi sur les droits d'auteur. Je pourrais vous en parler pendant des heures. Je dois m'y reporter énormément.

Je crois que ce serait une mesure très constructive si la Loi sur le droit d'auteur était modifiée pour tenir compte de cette technologie.

M. Fortier: Je crois que je puis répondre à votre question aussi en répétant, madame le président, ce que j'ai déjà dit tout à l'heure. Ce rapport vous vient directement du Sous-comité sur le droit, la science et la technologie sans avoir suivi le cheminement habituel de notre Association pour ce genre de mémoire. Le cheminement habituel comprend la diffusion d'un tel mémoire à toutes nos sections et à tous nos comités pour savoir ce qu'ils en pensent. Mais cette méthode aurait pris trop de temps et nous avons cru que vous vouliez savoir ce que nous avions à dire et avons donc décidé de venir ici maintenant pour faire le reste plus tard. Donc, en temps et lieu, nous saurons ce qu'en pensent des comités tels celui sur les brevets, les marques de commerce et les droits d'auteur. Cependant, cette étape n'a pas encore été franchie, monsieur.

M. Robinson (Etobicoke—Lakeshore): Je note que le mémoire a été présenté par une avocate qui a précisé à plusieurs reprises qu'elle s'intéresse à l'informatique plutôt qu'au droit criminel. Cependant, le mémoire semble surtout s'attaquer à l'aspect criminel.

Mme Kingston: Cela s'attaque plutôt à l'informatique.

[Text]

Mr. Bernard E. Blanchard (Member, Canadian Bar Association): Mr. Robinson, I am interested very much in the question that you have posed, as well as the one Mr. Beatty has posed, on the aspects of the Criminal Code. It seems to me there is a tendency today to isolate the indictable offences in the Criminal Code and rid it of all the ancillary—the other types of lesser offences; and I refer particularly to the principles and objectives of the Criminal Code that were published within the last year by the Minister of Justice; and also the Law Reform Commission, which has examined in totality the principles and objectives of the Criminal Code. I suggest that in keeping with that thinking, probably this kind of crime would be isolated outside the Criminal Code and statute law. This is a general feeling I have in this overall discussion.

But I think you will find that in due course the Criminal Code will be brought down to perhaps 150 or 100 or fewer articles dealing with serious, of course indictable, offences, and this type of crime, which will touch, as you have suggested, many areas and many different statutes, will be directed outside the Criminal Code. I think there is some tendency to that. This is, by the way, a recommendation of the Law Reform Commission of Canada.

Mr. Robinson (Etobicoke—Lakeshore): In the comments that were made earlier, the question of relating this so-called computer crime to the mischief section of the Criminal Code was pretty well ruled out. Do you not feel there could be a strengthening of that particular section of the Criminal Code, having different levels of criminality in the whole question of mischief; in other words, using mischief in its broadest sense and setting out a number of different sections under that?

Mr. Blanchard: I am sure it could be.

Mr. Robinson (Etobicoke—Lakeshore): So in your view, then, there are quite a number of sections in the Criminal Code itself that could be just changed, maybe significantly or even substantially, and that would cover the kind of thing we are concerned about when we are dealing computer crime.

Mr. Blanchard: Yes. With the present Criminal Code there is no doubt this could be done. But what I am suggesting particularly is that if any changes are operated within the whole concept of the principles and the objectives of the Criminal Code, then it is reasonable to assume the Criminal Code will eventually be rid of a number of sections which are not what we would call heavy crimes, or are not indictable offences and so on. I think there is a tendency to do that. But at the present time there is no doubt that several of these could fit into many of the 600 or so sections.

• 1705

Mr. Robinson (Etobicoke—Lakeshore): Yes. I noticed in your brief that there seemed to be a tendency to be super critical, but not necessarily to be super constructively critical. It seemed to me that this is less than helpful. I would have hoped that we would have had more suggestions with regard to the changes in definition, or changes that would be more properly presented, not only those that you have contained in

[Translation]

M. Bernard E. Blanchard (membre, Association du Barreau canadien): Monsieur Robinson, la question que vous venez de poser m'intéresse beaucoup, tout comme celle posée par M. Beatty pour ce qui a trait aux aspects du Code criminel. Il me semble qu'on tend aujourd'hui à circonscrire le Code criminel aux actes criminels pour en sortir les infractions de moindre importance; je me reporte plus précisément aux principes et objectifs du Code criminel publié il y a moins d'un an par le ministre de la Justice; aussi à la Commission de réforme du droit qui a étudié la globalité des principes et objectifs du Code criminel. Pour suivre ces exemples, je crois que ce genre de crime ne devrait pas tomber sous le coup du Code criminel ou du droit statutaire. C'est là l'esprit général qui se dégage, pour moi, de tout ce débat.

Cependant, je crois que vous trouverez qu'en temps et lieu le Code criminel ne se composera plus que de 150 ou 100 articles, ou moins encore, traitant de crimes sérieux et ce genre de crimes qui touchent, comme vous l'avez dit, à bien des domaines et à bien des lois différentes ne relèvera plus du Code criminel. Je crois qu'il y a une tendance à cela. Soit dit en passant, il s'agit là d'une recommandation de la Commission de réforme du droit du Canada.

M. Robinson (Etobicoke—Lakeshore): D'après ce qui a été dit plus tôt, il semble qu'on a décidé de ne pas lier le «crime ordinateursé» à la partie du Code criminel qui traite de méfait. Ne croyez-vous pas que l'on pourrait renforcer cette partie précise du Code criminel en y définissant divers niveaux de criminalité pour toute cette question de méfait; en d'autres termes, définir très largement ce qui constitue un méfait pour ensuite y apporter des précisions dans d'autres articles?

M. Blanchard: Je suis sûr qu'on pourrait le faire.

M. Robinson (Etobicoke—Lakeshore): Donc, d'après vous, il y a toute une série d'articles du Code criminel que l'on pourrait modifier, même quant au fond, et qui nous aideraient à régler le genre de problème qui nous préoccupe lorsqu'il s'agit du crime «informatisé».

M. Blanchard: Oui. Avec le Code criminel actuel, il ne fait aucun doute que cela pourrait se faire. Mais ce que je dis, plus précisément, c'est que s'il faut apporter des changements à l'intérieur même du concept global des principes et des objectifs du Code criminel, il est alors raisonnable de croire que le Code criminel sera éventuellement débarrassé d'un certain nombre d'articles se rapportant à des crimes que l'on ne conçoit pas être graves, qui ne sont pas des actes criminels et ainsi de suite. Je crois que c'est le genre de tendance qui se dessine. Cependant, à l'heure actuelle, il ne fait aucun doute que plusieurs de ces crimes pourraient s'insérer dans le cadre de beaucoup de ces quelque 600 articles.

M. Robinson (Etobicoke—Lakeshore): Oui. Je décèle dans votre mémoire une certaine tendance à la supercritique, mais pas nécessairement une critique superconstructive. Il me semble que c'est moins qu'utile. J'aurais osé espérer que vous nous auriez fait plus de propositions concernant des modifications à la définition ou des modifications qui auraient été mieux présentées, pas seulement celles qui se trouvent dans

[Texte]

your suggested draft section—394.(a)(1), where you define computer, computer program, computer software and computer system, but you have left out computer network, computer data, computerized data, firmware, data processing, digital and a number of other different areas that properly should be defined as well.

If we are dealing with this whole subject, I would think they should be addressed in the brief as well. Certainly they would have to be addressed when we are considering a piece of legislation or even amendments to the Criminal Code. Could each and every one of you or, at least one of you, comment on that?

Mr. Fortier: Mr. MacIntosh might lead the flurry of answers.

Mr. MacIntosh: As has already become evident this afternoon, almost any definition in this area is subject to criticism by others. It is very difficult to define some of these concepts, particularly in areas where there are changes. For instance, the definition that has been provided here for computer is one that has evolved through a number of other statutes. The other statutes came up with what, at the time, was considered to be a good definition of computer, but it was either overtaken by events or by legal thinking that indicated some weakness in that definition. This one we have come up with for computer I think will probably be good for about 10 years, which in this area is a pretty long life.

Mr. Fortier: Maybe the time it will take to pass an amendment!

Mr. Robinson (Etobicoke—Lakeshore): That might take a long time, if we are talking about amending the Patent Act, which I do not think has been amended for some 50 years. You know what happens, once an act is passed it usually remains carved in stone for generation after generation. It is very difficult to get the priorities in order to make any changes, whether they are insignificant or not, unless we have an omnibus bill, as we do each year in this regard.

Are you suggesting that your draft section is all-inclusive? Is this all the suggestion you are prepared to make with regard to change, to cover this whole question of computer crime? Is this all of it, or is this just touching the tip of the iceberg?

Mr. MacIntosh: I think perhaps I can answer that by saying what we did. We responded to the subject matter of Mr. Beatty's bill.

Mr. Robinson (Etobicoke—Lakeshore): You were content merely to look at the bill and come up with what you consider is a piece of draft legislation, or a section of the Criminal Code, that might cover the intent of the bill that was before us.

Mr. MacIntosh: Yes, we feel that this covers areas for which there is presently, out there, concern.

Mr. Robinson (Etobicoke—Lakeshore): I get the distinct impression that, because you have said it is difficult to come

[Traduction]

votre partie 394.a)(1) proposée où vous définissez ordinateur, programme d'ordinateur, logiciel et système d'ordinateur, mais où il ne se trouve rien quant aux réseaux d'ordinateurs, données d'ordinateur, micro-programmation, informatique, «digital» et nombre d'autres domaines où on devrait trouver des définitions aussi.

Si nous traitons de la globalité du sujet, j'imagine que l'on devrait en parler dans le mémoire aussi. Il faudrait certainement en parler lorsque nous étudions une loi ou même des modifications à apporter au Code criminel. Est-ce que chacun d'entre vous pourrait répondre à cette question ou au moins l'un d'entre vous?

M. Fortier: M. MacIntosh pourrait peut-être donner le coup d'envoi à ce qui sera une avalanche de réponses.

M. MacIntosh: Comme on l'a vu très clairement cet après-midi, presque toute définition donnée dans ce domaine est sujette à la critique des autres. IL est très difficile de définir certains de ces concepts surtout dans des domaines où tout change. Par exemple, la définition donnée ici pour le mot ordinateur en est une qui nous vient de plusieurs autres lois. Pour ces autres lois on avait trouvé ce qui semblait être à l'époque une bonne définition de l'ordinateur, mais elle a été dépassée soit par les événements, soit par la jurisprudence et on a donc décelé certaines faiblesses à cette définition. Cette définition du terme que nous avons trouvée vaudra probablement pour environ 10 ans, ce qui est quand même une longue période dans ce domaine.

M. Fortier: Cela prendra peut-être tout ce temps-là pour adopter un amendement!

M. Robinson (Etobicoke—Lakeshore): Cela pourrait prendre beaucoup de temps s'il s'agit de modifier la loi sur les brevets qui n'a pas été modifiée une seule fois depuis quelque 50 ans. Vous savez ce qui arrive: quand une loi est adoptée, elle est, pour ainsi dire, gravée dans la pierre pour des générations après générations. Il est très difficile de bien ordonner toutes les priorités pour faire les modifications qui s'imposent, qu'elles soient insignifiantes ou non, à moins de présenter un projet de loi omnibus comme nous le faisons chaque année à cet égard.

Voulez-vous dire que votre proposition est complète? Ce sont là les seules propositions de modifications que vous allez nous présenter concernant toutes ces questions de crime informatisé? Est-ce que c'est tout ou est-ce que c'est seulement la partie apparente de l'iceberg?

M. MacIntosh: Je crois que je pourrais peut-être répondre en précisant quelle fut notre démarche. Nous avons réagi au sujet du projet de loi de M. Beatty.

M. Robinson (Etobicoke—Lakeshore): Vous avez tout simplement lu le projet de loi pour ensuite proposer des amendements au Code criminel qui tiendraient compte des préoccupations soulevées.

M. MacIntosh: Oui, nous croyons que cela répond aux problèmes qui existent à l'heure actuelle.

M. Robinson (Etobicoke—Lakeshore): J'ai la nette impression que vous seriez tout à fait prêts à laisser la décision

[Text]

up with definitive statements defining some of the terms that are used in the computer industry, you would be prepared to leave it up to the judge or the courts to define. I would suggest to you that that is not good enough. Hopefully, we would not have to go to court in order to get definitions of things. We should have it properly stipulated in the legislation as to what we are talking about, so that we do not always have to go to court to find out. That may be the American system, it certainly is not the British system, and I would hope that it is not our system. Would you care to comment on that?

Mr. MacIntosh: You said that we indicated that it was difficult to define. I think it is impossible to define some of these terms in a meaningful way, which it is going to be meaningful to a court without somebody there to guide them as to what the words mean. If they are going to bring in experts to tell them what the words mean, they do not need the definition in the section, the definition in the section is not going to be that helpful. Some of the American statutes have eight or ten or twelve definitions dealing with this topic and we kind of wonder why they are doing it. They are so convoluted and they are so technically oriented that I would suggest that they were drawn by computer people, rather than by lawyers. As a result, the courts are going to have to call in experts to find out what is data. In the context of what is going on in a particular operation, what is data? What does it mean?

• 1710

Mr. Robinson (Etobicoke—Lakeshore): I appreciate your comments, Mr. MacIntosh, but you said it is impossible. If you look in *The Shorter Oxford Dictionary* as to the meaning of the word "impossible", it really means that it is difficult. So we are just going around in a circle. I do not think because we say it is difficult or it is impossible that it cannot be done. I think we have to keep working at it.

Going back to *Alice in Wonderland*, when you use a word it should mean what you say it means, not anything more or anything less. I think we have to reach that conclusion. We should not just leave it up to the courts to decide or to wring their hands and say they cannot make a decision. We have to be...

Mr. Fortier: With the greatest of respect, there is here an attempt—it may be a weak one—at definitions of "computer", "computer program", "computer software" and "computer system", and it is an attempt which this committee has come up with after looking at various solutions in that jurisdiction south of the border where attempts have been made. So, rightly or wrongly, this is our best effort at the moment. We are not saying that it is impossible; we are saying that it is possible, and here it is. It may not be satisfactory because of the rapid growth of this whole area, but here is our best attempt as of June 1983.

[Translation]

au juge ou aux tribunaux parce que vous avez dit qu'il est difficile de trouver des définitions définitives pour certains termes dont on se sert dans l'industrie de l'ordinateur. Très respectueusement, cela ne fait pas le poids. J'ose espérer que nous n'aurons pas à nous en remettre aux tribunaux pour que soient établies certaines définitions. Il faudrait que tout soit bien stipulé dans la loi afin que nous n'ayons pas toujours à recourir aux tribunaux pour les définitions. C'est peut-être là le système américain, mais ce n'est surtout pas le système britannique et j'ose espérer que ce n'est pas notre système. Qu'en pensez-vous?

M. MacIntosh: Comme vous l'avez signalé, nous avons dit qu'il était difficile de trouver des définitions. Je crois qu'il est impossible de définir certains de ces termes de façon à ce que la définition soit utile à un tribunal sans que ce dernier n'ait besoin de recourir à quelqu'un pour expliquer la signification des mots. Si le tribunal doit avoir recours à un expert pour se faire expliquer la définition, point n'est besoin d'inclure la définition dans cette partie, car elle ne sera pas vraiment utile. Dans certaines des lois américaines, on trouve 8 ou 10 ou 12 définitions traitant de ce sujet et nous nous demandons vraiment quelle en est l'utilité. Ces définitions sont si tordues et si techniques qu'il me semble qu'elles ont été rédigées par des experts en informatique plutôt que par des avocats. Résultat, les tribunaux devront faire appel à des experts pour savoir ce qui constitue une donnée. Dans le contexte de ce qui se passe pendant une opération précise, qu'est-ce qui constitue une donnée? Que signifie ce terme?

M. Robinson (Etobicoke—Lakeshore): Je comprends ce que vous dites, monsieur MacIntosh, mais vous avez dit que c'était impossible à faire. Si vous vous reportez au *The Shorter Oxford Dictionary* pour savoir ce que signifie le mot «impossible», vous verrez que cela signifie tout simplement que c'est difficile. Donc, nous ne faisons que tourner en rond. Ce n'est pas parce que nous disons qu'une chose est difficile ou impossible que cela ne peut se faire. Je crois qu'il nous faut continuer d'y travailler.

Pour retourner à *Alice au pays des merveilles*, lorsque vous vous servez d'un mot, il faudrait que ce mot signifie ce qu'il signifie, pas plus, pas moins. Je crois qu'il nous faut en arriver à cette conclusion. Nous ne devrions pas tout simplement laisser les tribunaux trancher la question ou gémir d'angoisse en disant qu'ils ne peuvent prendre de décision. Nous devons...

M. Fortier: Avec le plus grand respect, on essaie quand même, même si l'effort est peut-être faible, de définir «ordinateur», «programme», «logiciel» et «système d'ordinateur»; le comité propose ces définitions après avoir étudié certaines solutions employées par nos voisins du sud. Donc, à tort ou à raison, c'est ce que nous avons fait de mieux jusqu'ici. Nous ne disons pas que c'est impossible; nous disons que c'est possible et voici les résultats. Ce n'est peut-être pas satisfaisant à cause de la croissance rapide que connaît tout le secteur, mais au mois de juin 1983, c'était ce que nous pouvions faire de mieux.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): I agree with you that you have an attempt here, and I can only say that at the moment I can properly accept the four definitive terms that you have with the definitions that go along with them. But for our purposes all I am throwing out to you is that we do not think . . . at least I personally do not think—that is going far enough. We need a lot more assistance than that. If you can come back with some more definitions that would be helpful to us, maybe we would see that they could be incorporated in the legislation, whatever it may be. We need all the help we can get in this matter, and that is why we are looking to people like the Canadian Bar Association to be of whatever assistance you can.

Mr. Blanchard: I do not think the mandate that was given to the Law Science and Technology Section was to prepare a model bill; I think it was, rather, to respond to Bill C-667. Perhaps from the outside the outlook of the committee was quite different from what you are suggesting. If it had been to prepare a model bill, I think perhaps the bar could have done this; but it was not the mandate given to it.

The Chairman: Maybe you could come back. You said previously that there are other committees that normally would be consulted. Can we expect these committees, then, to give their reactions to our report—because obviously our report will be tabled before your committees will have time to react . . . and maybe come back at a later date this year with some suggestions, knowing very well that our report will be just part of the documentation or whatever, support information, for the ministry to prepare the final bill? So maybe you could give us the procedure within your own organization and when you could come up with maybe a more comprehensive suggestion from the bar on the larger and broader aspects of computer crime.

Mr. Fortier: Yes, with pleasure. Indeed, if I may, before I give you any kind of a timetable, ask respectfully for your timetable. You are going to report when?

The Chairman: Before the session ends, and this session will end June 30.

Mr. Fortier: Yes.

The Chairman: We intend to table our report in about 10 or 12 days. Of course, you have the rest of the summer. I do not expect any legislation coming from the government before next fall, which means that you could have time to react to our report and of course be able to deal with other aspects that will be included in our report.

Mr. Fortier: And we will.

Ms Kingston: Would you intend any response from the Canadian Bar Association to include aspects of law other than the criminal aspects?

[Traduction]

M. Robinson (Etobicoke—Lakeshore): Je suis bien d'accord pour dire avec vous que vous avez fait un effort et je ne puis que dire que je puis accepter les quatre termes définitifs que vous nous proposez avec les définitions. Mais, pour nos fins, tout ce que je vous dis, c'est que nous ne croyons pas, du moins je ne crois pas personnellement, que vous êtes allés assez loin. Il nous faudra beaucoup plus d'aide que cela. Si vous pouviez nous revenir avec plus de définitions qui pourraient nous être utiles, peut-être pourrions-nous faire en sorte qu'elles fassent partie de la loi, quelle qu'elle soit. Nous avons besoin de toute l'aide qu'on peut nous donner en la matière et c'est pourquoi nous nous tournons vers des organismes comme le vôtre, l'Association du Barreau canadien, et vous demandons de donner toute l'aide dont vous êtes capables.

M. Blanchard: Je ne crois pas que le mandat donné à notre comité sur le droit, la science et la technologie était de préparer un projet de loi modèle; je crois plutôt qu'on leur a dit tout simplement de répondre au projet de loi C-667. De l'extérieur, peut-être le comité a-t-il vu les choses d'un oeil différent du vôtre. S'il avait fallu préparer un projet de loi modèle, je crois que peut-être le Barreau aurait pu le faire; cependant, ce n'est pas le mandat qui lui a été confié.

Le président: Peut-être pourriez-vous revenir. Vous avez dit plus tôt que vous auriez habituellement consulté d'autres comités. Pouvons-nous nous attendre, donc, à ce que ces comités fassent savoir ce qu'ils pensent de notre rapport, car il est évident que notre rapport sera déposé avant que vos comités n'aient eu le temps de réagir à la chose, et vous pourriez peut-être revenir un peu plus tard cette année avec d'autres propositions sachant fort bien que notre rapport ne sera qu'une partie de toute la documentation sur laquelle se fondera le ministère pour préparer le projet de loi final? Alors peut-être pourriez-vous nous faire connaître la procédure au sein de votre organisme et le Barreau pourrait peut-être alors nous faire parvenir des propositions plus globales quant aux aspects les plus larges et les plus généraux de toute cette question des infractions relatives aux ordinateurs.

M. Fortier: Oui, avec plaisir. Avant de vous faire connaître un échéancier quelconque, pourrais-je vous demander le vôtre? Quand votre rapport sera-t-il présenté?

Le président: Avant la fin de la présente session qui se termine le 30 juin.

M. Fortier: Oui.

Le président: Nous entendons déposer notre rapport dans 10 ou 12 jours environ. Evidemment, vous avez le reste de l'été. Je ne crois pas que le gouvernement présente de projet de loi avant l'automne prochain, ce qui signifie que vous auriez le temps voulu pour étudier notre rapport et traiter aussi d'autres aspects qui s'y trouveront.

M. Fortier: Ce que nous ferons.

Mme Kingston: Dans les documents qui viendraient éventuellement de l'Association du Barreau canadien, voudriez-vous trouver quelques commentaires sur des aspects de la loi autres que ce qui touche le criminel?

[Text]

Mr. Robinson (Etobicoke—Lakeshore): Pardon me for interrupting. I think we certainly want to know what you are thinking about the changes or recommendations for change in the Canada Evidence Act.

Mr. Fortier: That is definitely going forward. On June 22 we are appearing before a committee in another place with a comprehensive, over 200-page brief. That is Bill S-33, proposed amendments to the Canada Evidence Act. One of our 15 chapter submissions is on the evidentiary impact of the proposed changes relating to computer.

• 1715

Mr. Beatty: Also the question of copyright, if you felt it was relevant, I think should be included in your response to the committee.

Ms Kingston: With respect to criminal aspects only or civil rights as well?

Mr. Beatty: No, any... The mandate of this committee is very broad because the subject matter of my bill, namely, computer crime, was referred to the committee and we have cast our net quite broadly; we are interested in anything related to computer crime that would be helpful. It is not the letter of the bill that is before us; it is the subject matter.

Ms Kingston: Oh, I thought it was only criminal offences.

Mr. Fortier: As I explained in my opening remarks, Madam Chairman, we are here to answer a specific narrow question and without having followed our usual process of consultation with all other sections and committees of the bar. This process is now in... I have pushed the button and the sausage machine is churning. So in due course we will have this multidisciplinary brief which will address, I hope, all of your legitimate concerns.

The Chairman: Well, maybe it is always easy to explain how we work and, of course, you could react to a government bill at a later date...

Mr. Fortier: Oh, yes.

The Chairman: —or you could give your advice before the bill is tabled. As parliamentarians, we always say if you want to have the best input it is prior to the passage of a bill, rather than afterwards, because it is always easier to orient in one direction once you have the input beforehand. That is why we say, since the machine has already started working and you have some work done, our suggestion—and I think this is my colleagues' point of view too—would be that if early next fall we could have your report from your various branches and other committees, the criminal law one and the one that is dealing with other aspects of the bill, and could have a chance to have a look and give their advice on our report—and you will see that we are dealing also with the privacy law. We are dealing with a very wide range of legislation, because all that

[Translation]

M. Robinson (Etobicoke—Lakeshore): Désolé de vous interrompre. Je crois que nous voudrions certainement savoir ce que vous pensez des modifications proposées actuelles ou à venir à la Loi sur la preuve au Canada.

M. Fortier: Cela sera certainement fait. Le 22 juin, nous comparaissons devant un comité du Sénat et nous allons déposer un mémoire de plus de 200 pages. Le sujet en est le projet de loi S-33, modifications proposées à la Loi sur la preuve au Canada. Un de nos 15 chapitres porte sur les répercussions des changements proposés en matière d'ordinateurs sur la Loi sur la preuve.

M. Beatty: Pour ce qui est du droit d'auteur, si vous pensez que cette question a un rapport, je crois qu'il faudrait en parler dans vos réponses au Comité.

Mme Kingston: Par rapport au droit criminel seulement ou aussi les aspects civils?

M. Beatty: Sous tous les angles... Le mandat de notre Comité est très vaste et concerne le sujet de mon projet de loi, c'est-à-dire les infractions contre les droits de propriété relatifs aux ordinateurs, ce qui englobe beaucoup de choses; nous aimerions connaître tous les aspects de ces infractions susceptibles de nous intéresser. Nous ne nous limitons pas aux seules dispositions du projet de loi: c'est le sujet dans son ensemble qui nous intéresse.

Mme Kingston: Oh, je pensais que c'était seulement les infractions criminelles.

M. Fortier: Comme je l'ai expliqué dans mes remarques préliminaires, madame le président, nous comparaissons ici pour parler d'une question précise assez restreinte sans avoir suivi notre procédure habituelle de consultation avec tous les autres comités et sections du Barreau. Le mécanisme a été mis en branle et tout le processus a été activé. Nous aurons donc en temps voulu un mémoire multidisciplinaire qui traitera, j'espère, de tous les points qui vous intéressent.

Le président: Eh bien, je devrais peut-être expliquer comment fonctionne le Comité et vous pourriez bien sûr répondre à un projet de loi du gouvernement qui serait présenté à une date ultérieure...

M. Fortier: Certainement.

Le président: ... ou vous pourriez faire connaître vos opinions avant le dépôt du projet de loi. Comme parlementaires, nous sommes d'avis que la contribution la plus utile vient toujours avant l'adoption d'un projet de loi, plutôt qu'après, car il est certainement plus facile d'orienter les choses dans une direction donnée au moment de la discussion préliminaire. Puisque vous dites que le mécanisme a été mis en branle et que vous avez déjà accompli un certain travail, je crois qu'il nous serait utile de recevoir au début de l'automne prochain le rapport de vos diverses divisions et de vos autres comités, celui qui s'occupe du droit criminel et celui qui s'intéresse aux autres aspects du projet de loi. Nous pourrions aussi entendre vos opinions et vos conseils concernant notre rapport—et vous constaterez que nous considérons la Loi sur la protection de la

[Texte]

technology has touched on so many aspects of everybody's life that we at least want to give to our colleagues in Parliament the correct perspective of the problem, not just the computer crime aspect, but just outlining to them how wide this question is and how much it is affecting everybody's life. That is why we are touching on more than just one narrow aspect of Mr. Beatty's bill.

M. Blanchard: Madame le président, si je comprends bien, votre rapport sera soumis avant ou vers le 30 juin.

Le président: Oui, le 23 juin.

M. Blanchard: Serait-il possible, à ce moment-là, d'avoir accès à ce rapport afin que nous puissions, à notre tour, y répondre?

Le président: Ce sera déposé à la Chambre. Il s'agit d'un rapport officiel qui sera déposé à la Chambre des communes et qui sera entériné par le Comité de la justice et des questions juridiques. Il sera rendu public et les greffiers se feront un devoir de le faire parvenir en tout premier lieu à ceux qui auront comparu. Par la suite, ils en feront la distribution habituelle, mais les copies additionnelles seront remises à ceux qui voudront se servir du rapport comme outil de travail.

M. Blanchard: Très bien, je vous remercie.

The Chairman: Mr. Robinson, would you like to conclude?

Mr. Robinson (Etobicoke—Lakeshore): Yes, I will be very short.

In defining "computer" one of our witnesses made the statement that it is what it does, not what it is, and this is a rather trite statement to say the least. What you are really saying is that a thing is what it does and I am wondering if there is any limitation to this or, at the present time do you think that computer as you understand it, and you have put the term in quotes, is just that? What it does is what it is. Is that a finite statement?

Mr. MacIntosh: Well, that was my definition. I am afraid I do not quite get the impact of your question though.

Mr. Robinson (Etobicoke—Lakeshore): Well, maybe I can try again. You were defining the computer and various things that a computer does, so you made the statement that it is what it does. It is not the physical instrument itself or the piece of equipment itself but what you get out of that equipment or what it does itself, or what it creates.

• 1720

Mr. MacIntosh: Perhaps we could look at the definition. It means an internally programmed general purpose device, capable of automatically accepting data processing, data supply and the results of the operation, which places the emphasis upon the function the computer performs rather than in other definitions. For instance, the one in the bill we have under discussion is: "any programmable device or apparatus designed to store or process data or information".

[Traduction]

vie intime. Nous devons considérer une vaste gamme de lois dans la mesure où cette technologie touche tant d'aspects de la vie quotidienne de tout le monde. Nous tenons à présenter à nos collègues une perspective adéquate de la question, pas seulement ce qui touche les infractions contre les droits de propriété relatifs aux ordinateurs, pour qu'ils se rendent compte de l'étendue de cette question et la façon dont elle se répercute sur la vie de tout le monde. C'est pour cette raison que nous ne nous limitons pas au champ restreint du projet de loi de M. Beatty.

Mr. Blanchard: Madam Chairman, if I understand correctly, your report will be submitted before or around June 30.

The Chairman: Yes, June 23rd.

Mr. Blanchard: Would it be possible for us to consult the report at that time so that we can respond?

The Chairman: It will be tabled in the House. It is an official report which will be tabled in the House of Commons and sanctioned by the committee on Justice and Legal Affairs. It will be made public and the clerks will make a point of sending a copy to all witnesses. Afterwards, there will be the usual distribution but additional copies will be sent to those who will be using the report as a working instrument.

Mr. Blanchard: Thank you.

Le président: Monsieur Robinson, voulez-vous prendre la parole comme dernier intervenant?

M. Robinson (Etobicoke—Lakeshore): Oui, je serai très bref.

Dans sa définition de l'ordinateur, l'un de nos témoins a dit que l'important c'est ce qu'il fait, non pas ce qu'il est, affirmation assez banale pour dire le moins. Cela revient à dire qu'une chose est ce qu'elle fait et je me demande si on peut imposer des limites à cela ou bien à l'heure actuelle pensez-vous que «l'ordinateur» se définit tout simplement de cette façon? Ce qu'il fait est ce qu'il est. Cela comporte-t-il des limites?

M. MacIntosh: Eh bien, c'était ma définition. Malheureusement je n'ai pas bien saisi le sens de votre question.

M. Robinson (Etobicoke—Lakeshore): Je vais essayer encore une fois. Vous donniez une définition de l'ordinateur et des différentes choses qu'il fait, vous avez dit qu'il est ce qu'il fait. Ce n'est pas l'instrument physique comme tel ni l'équipement mais ce que cette machine vous donne ou ce qu'elle fait elle-même ou ce qu'elle crée.

M. MacIntosh: On pourrait peut-être étudier la définition. Il s'agit d'un dispositif polyvalent programmé capable de traiter et de fournir des données et de faire des opérations. Cela met l'accent sur la fonction de l'ordinateur contrairement à d'autres définitions. Par exemple, la définition proposée dans le projet de loi est la suivante: «tout appareil ou dispositif informatisé destiné à emmagasiner ou à traiter de l'information».

[Text]

Mr. Robinson (Etobicoke—Lakeshore): All right, I will leave that aspect of it and go on to something else.

Do you have any suggestions to make with regard to the protection of what may be contained in the computer? What do you recommend with regard to the protection of the computer system, the computer programs, the computer software?

Mr. MacIntosh: Our bill proposes that it be made a criminal offence to obtain use of the computer system or to alter or destroy a computer program. "Computer system" and "computer program" are both given extended meanings so that they cover not only the physical machine itself but the software resident within it and software which is not resident in it but is intended to be used in it.

Mr. Robinson (Etobicoke—Lakeshore): On page 10 of the dissertation, you talk about types of computer abuse and you enumerate a, b, c, d, e and f. Then the statement is made:

Each of the subdivisions just noted, represents in reality problems which have long existed, but when they existed without the use of a computer, the problems were not regarded in the same light.

I wonder what you really mean by this, particularly the words "without the use of a computer". Could you explain that more fully?

Mr. MacIntosh: These several pages are a quote from Frank Spitzer, who filed a brief previously at another conference dealing with this same topic. I think what he is talking about is that these were recognized as problems, and some attempt was made to allocate this type of misconduct under various provisions of the Criminal Code with indifferent success.

Mr. Robinson (Etobicoke—Lakeshore): The thing I really object to is this. Because there is no law in place that specifically makes computer crime a computer crime, shall we say, there is a tendency, as is stated here on this page, to bend the law in order to satisfy the problem. That certainly does not look like justice; and I find it rather unusual, even though this is a comment made in quotes, that it would even be used by the Canadian Bar Association, that we would think we would bend the laws in order to satisfy the problem. We are usually looking for every technicality there is to avoid the law.

Mr. MacIntosh: I think the problem being got at there is that two things are happening. The judges, who may not have a very high technical background, have these cases thrown at them and misapprehend, even after listening to evidence, just what the equipment really has been doing, and hence, make a legal decision which does not accord with the facts as they did happen. On the other hand, seeing that something wrong has occurred, there is a tendency on the part of some courts to, let us say, define or re-define a word so that particular type of misconduct is covered.

Mr. Robinson (Etobicoke—Lakeshore): On page 13 of your statement, in paragraph 6 under penalty, you say: "Computer crime ranges from the serious to the ridiculous". So this brings

[Translation]

M. Robinson (Etobicoke—Lakeshore): Très bien, je vais laisser cet aspect et passer à autre chose.

Avez-vous des suggestions à faire concernant la protection de ce que peut contenir l'ordinateur? Que recommandez-vous en ce qui concerne la protection du système informatisé, les programmes de l'ordinateur et le logiciel?

M. MacIntosh: Notre projet de loi propose que le fait de se servir d'un système informatique ou la modification ou la destruction d'un programme informatique deviennent une infraction criminelle. On donne un sens élargi aux termes «système informatique» et «programme informatique» pour qu'ils s'appliquent non seulement à la machine elle-même mais aux logiciels qu'elle contient et aux logiciels qu'elle ne contient pas mais qui sont destinés à y être programmés.

M. Robinson (Etobicoke—Lakeshore): A la page 2 de votre mémoire, vous parlez de différentes sortes d'abus de l'informatique et vous énumérez une série d'exemples. On dit ensuite:

Chacune de ces sous-divisions représente en fait des problèmes qui existent depuis longtemps mais sans les possibilités offertes par l'informatique, ils n'étaient pas considérés sous le même angle.

Qu'entendez-vous par cela, surtout quand vous dites «sans les possibilités offertes par l'informatique»? Pourriez-vous nous expliquer?

M. MacIntosh: Ce sont plusieurs pages tirées d'un mémoire présenté par Frank Spitzer lors d'une conférence qui portait sur ce sujet. Je crois qu'il reconnaît que cette question posait déjà des problèmes et qu'on a essayé de prévoir ce genre d'inconduite, avec peu de succès, dans différentes dispositions du Code criminel.

M. Robinson (Etobicoke—Lakeshore): Voici la chose qui me dérange. Puisque la loi ne prévoit pas de façon précise les crimes impliquant l'informatique ou l'ordinateur, on a tendance, comme vous constatez ici, d'infléchir la loi pour qu'elle puisse répondre à ce genre de situation. Cela ne donne certainement pas l'apparence de justice et je m'étonne qu'une observation semblable, même s'il s'agit d'une citation, soit faite par l'Association du Barreau canadien, qu'on invoque cette idée d'infléchir la loi afin de répondre au problème. D'habitude, on cherche tous les points techniques qui permettent d'éviter le recours à la loi.

M. MacIntosh: À mon avis, le problème évoqué ici concerne deux choses. Les juges, ayant peut-être des connaissances techniques peu développées, doivent entendre ce genre de cause et même après l'exposé des preuves ils comprennent mal comment l'équipement a été utilisé et, par conséquent, prennent une décision juridique qui ne correspond pas aux faits réels. D'autre part, certains tribunaux reconnaissant qu'un méfait a été commis, ont tendance à définir un terme, ou à donner une nouvelle définition, de façon à ce qu'il s'applique au cas visé.

M. Robinson (Etobicoke—Lakeshore): A la page 13 de votre déclaration, au paragraphe 6 concernant la sanction, vous dites: «les infractions contre le droit de propriété relatif aux ordinateurs englobent aussi bien des crimes graves que des

[Texte]

up the whole question of the proposed section we were talking about before on mischief.

Then you go on to say:

For this reason, the authorities should have the option to lay a charge as either an indictable offence or a summary conviction offence.

So this would really set different categories, as I was suggesting, under the proposed mischief section of the Criminal Code.

But I am wondering if there is another category here. What about the option not to lay charges at all? We had The Canadian Bankers' Association before us, and they did not think any charges should be laid at all in most cases. They did not consider there was such a thing as computer crime, as far as they were concerned, although they limit it to the banking system. But should there be the option on the individual to either report the computer theft or the crime, or do you think this should be just left up to the authorities, the police, in their police work to detect the crime and then lay the charges? How do you think this should be handled?

• 1725

Mr. Fortier: Let me give a general answer, if I may, and then the experts can speak, but that option always exists. The Crown prosecutor always has the option of laying a charge or not.

Mr. Robinson (Etobicoke—Lakeshore): It could be a private complaint.

Mr. Fortier: In most jurisdictions private complaints need the endorsement or the authorization or the fiat, if you wish, of the attorney general.

Mr. Robinson (Etobicoke—Lakeshore): If you wanted to register a complaint, you would go before a justice of the peace and provide him with sufficient information whereby he thinks that a crime has been perpetrated or a charge should be laid, and not necessarily the police.

Ms Kingston: I think to some extent . . . even though this is the area I practise in, there seems to be undue concern in all aspects of law, and other aspects, with respect to computers. With respect to law, there seems to be a big concern that just because there is a hole there it must be covered in certain ways, which is not necessarily the case, that there has to be specific exceptions just for computers, which is not necessarily the case either. I think this reporting requirement may be one such instance. I think if you were to require people to report any instance of a crime with respect to computers, it would be a folly idea. If you were going to have such a requirement, that requirement should be uniform in the act, and then you would run into all kinds of situations. For example, if I just go like this, have I committed an assault on you? I could, because he may have a thought in his head that I could carry that punch out and really hurt him, in which case I may have assaulted him. Should he now be required to go to the police? And if he does not, is he in violation?

[Traduction]

cas ridicules». Cela nous mène à l'article proposé concernant le méfait.

Vous dites plus loin:

Pour cette raison, les autorités devraient pouvoir porter plainte pour un acte criminel ou bien une infraction faisant l'objet d'une déclaration sommaire de culpabilité, selon le cas.

Il s'agirait donc d'établir des catégories différentes, comme je le suggérais, en vertu de la proposition concernant l'article du Code criminel qui porte sur le méfait.

Mais je me demande s'il n'existe pas une autre possibilité ici, c'est-à-dire l'option de ne pas porter plainte? Nous avons entendu l'Association des banquiers canadiens qui était d'avis qu'il n'était pas nécessaire de poursuivre en justice dans la plupart des cas. Elle ne pensait pas qu'il existait des infractions contre les droits de propriétés relatifs aux ordinateurs, en ce qui la concernait, c'est-à-dire les observations bancaires. A votre avis, le citoyen devrait-il avoir l'option de signaler le vol ou l'infraction impliquant l'ordinateur ou devrait-on laisser à la police le soin de découvrir l'infraction et de porter ensuite les accusations? Selon vous, comment devrait-on procéder?

M. Fortier: Je vais vous répondre de façon générale, si vous permettez, et laisser ensuite répondre les spécialistes. C'est une option qui existe toujours. Le procureur de la Couronne a toujours la possibilité d'inculper ou de ne pas le faire.

M. Robinson (Etobicoke—Lakeshore): Il pourrait s'agir d'une plainte d'un particulier.

M. Fortier: Dans la plupart des cas, les plaintes déposées par un particulier doivent être approuvées par le procureur général.

M. Robinson (Etobicoke—Lakeshore): Si on voulait déposer une plainte, il suffirait de donner à un juge de paix des renseignements suffisants pour qu'il croit qu'un crime a été perpétré et qu'une accusation est justifiée, sans forcément s'adresser à la police.

Mme Kingston: Même si c'est le domaine du droit dans lequel j'exerce, je crois qu'il existe des inquiétudes non justifiées à l'égard des ordinateurs, en ce qui a trait à tous les aspects de la loi. On semble croire que, parce qu'il existe un trou, il faut le combler de différentes façons, ce qui n'est pas forcément le cas, qu'il faut des exceptions précises pour l'ordinateur, ce qui n'est pas forcément le cas non plus. Je crois que cette exigence relative du signalement d'une infraction est un bon exemple. Si on devait obliger les gens à signaler tous les cas d'une infraction touchant les ordinateurs, ce serait une aberration. Une telle exigence devrait être uniforme dans la loi et on se trouverait devant toutes sortes de situations. Par exemple, si je fais ce geste menaçant, suis-je coupable d'une agression? Peut-être, car il aurait pu penser que j'avais l'intention d'y donner suite et, effectivement, lui donner un coup de poing pour lui faire mal, auquel cas j'aurais pu être coupable d'une agression. Devrait-il être tenu d'en faire rapport à la police? Et s'il ne le fait pas, contrevient-il à la loi?

[Text]

Mr. Robinson (Etobicoke—Lakeshore): No. It might be assault, but not a battery.

Ms Kingston: I think you are going to run into all kinds of problems which are going to create an administrative nightmare.

Mr. Robinson (Etobicoke—Lakeshore): It can be absolutely horrendous, that is true. But the point I was really trying to get at was whether you thought in fact there should be compulsory reporting or whether you would just leave that out.

Ms Kingston: I would definitely leave that out.

Mr. Robinson (Etobicoke—Lakeshore): All right, even though we are coming into that sort of thing more and more all the time—for instance, child abuse. Now you are required to report any instance of child abuse. Where do you draw the line? How much abuse are we talking about? Just recently a doctor was charged or up before his colleagues, I suppose, for not reporting child abuse. We are getting into this whole area, because it is so serious.

Now, if you are saying that computer crime is not a serious matter, it does not have to be reported and so on, then fine, that is your approach. But I just wonder—how serious is it? You are not putting it in the same category as child abuse, that is for sure, but how far do we go in this?

Mr. Fortier: The way we have addressed it is by saying that we acknowledge there can be serious and less serious computer crimes. For that reason, and this is not a choice which is found very often in the present Criminal Code, we say there should be this alternative of either proceeding by way of summary conviction or by way of an indictable offence. That is how we answer the wide spectrum of the severity or the seriousness of the particular computer crime.

Mr. Robinson (Etobicoke—Lakeshore): That takes away your suggestion of triviality, then, does it not?—by having offences classified as to whether they are indictable or summary.

Mr. Fortier: There are some trivial offences, like mischief, for example, which still end up and still, in my personal view, should end up in the criminal courts.

The Chairman: Your last question.

Mr. Robinson (Etobicoke—Lakeshore): Okay, I guess I have only one question. I would like to have a few more but my colleague took so much of my time . . .

Mr. Beatty: I apologize. I thought it was because you were late getting . . .

Mr. Robinson (Etobicoke—Lakeshore): My final question, then, will be—oh, I have to really bootleg two of them in here. I wanted to know what you thought about the whole question of security. There is an article in the May 20, 1983, edition of

[Translation]

M. Robinson (Etobicoke—Lakeshore): Non. C'est peut-être un cas d'agression, mais pas des voies de fait.

Mme Kingston: Je crois que vous allez vous heurter à toutes sortes de difficultés qui créeront un cauchemar administratif.

M. Robinson (Etobicoke—Lakeshore): Je reconnais que cela peut donner lieu à quelque chose d'épouvantable. Mais je cherchais à savoir si vous pensez qu'il faudrait obliger les personnes à signaler ces cas ou vaudrait-il mieux ne rien prévoir de semblable?

Mme Kingston: Je préférerais certainement qu'une telle disposition n'existe pas.

M. Robinson (Etobicoke—Lakeshore): Très bien, même si c'est un genre de disposition qui devient de plus en plus fréquente . . . par exemple, les mauvais traitements infligés aux enfants. On est maintenant tenu de signaler tous les cas de mauvais traitements des enfants. Où établit-on la limite? Quelle doit être la gravité de ces sévices? Récemment, un médecin a été obligé de se justifier devant ses collègues parce qu'il n'avait pas signalé un cas de mauvais traitement d'un enfant. Nous essayons de faire quelque chose dans ce domaine parce qu'il est tellement sérieux.

Or, si vous pensez que les infractions reliées à l'ordinateur ne sont pas des questions sérieuses et qu'il ne faut pas les signaler, c'est votre droit. J'aimerais savoir quelle importance vous y accordez. Vous ne mettez pas ces infractions dans la même catégorie que les sévices infligés aux enfants, mais jusqu'où faut-il aller?

M. Fortier: Nous reconnaissons qu'il peut y avoir des infractions graves dans ce domaine et de moins graves. Pour cette raison, et ce n'est pas un choix qui est offert souvent dans le Code criminel actuel, nous disons qu'il faudrait avoir la possibilité de choisir entre une procédure de déclaration sommaire de culpabilité ou une accusation d'un acte criminel. C'est ainsi que nous serions en mesure de réagir de façon appropriée à la gravité d'une infraction particulière.

M. Robinson (Etobicoke—Lakeshore): Cela semble donc écarter la possibilité que vous évoquez d'infractions insignifiantes, c'est-à-dire le classement des infractions que vous venez de proposer.

M. Fortier: Il y a certaines infractions sans gravité, comme le méfait qui relève des cours criminelles et qui devrait, à mon avis, continuer d'en relever.

Le président: Votre dernière question.

M. Robinson (Etobicoke—Lakeshore): Il ne me reste qu'une question. J'aimerais en poser quelques autres, mais mes collègues ont pris tellement de mon temps . . .

M. Beatty: Je m'excuse. Je pensais que c'était parce que vous étiez en retard . . .

M. Robinson (Etobicoke—Lakeshore): Voici ma dernière question . . . en fait, je vais en poser deux. Je voulais savoir ce que vous pensez de toute cette question de la sécurité. On trouve un article dans le numéro du 20 mai 1983 du *Ontario*

[Texte]

the *Ontario Lawyers' Weekly*—I do not know whether you people read that mundane publication.

Mr. Fortier: Yes.

Mr. Robinson (Etobicoke—Lakeshore): It is entitled *Software Insecurities—Computer Programs and the PPSA*—which stands for Personal Property Security Act. I would like to have some comment on that. Maybe you know something about it and you would like to comment on that.

• 1730

Also, would you care to comment on the question of the code of ethics, involving computers and computer data processing and that kind of thing? I see Ms Kingston is nodding her head "yes" and smiling greatly.

Ms Kingston: About the article, unfortunately it is clipped on my desk but I have not read it, so I cannot respond to the article.

About security in general, given this is your wide mandate, I think it would be very definitely an area you should look into. It could be somehow incorporated into making certain things an offence in the Criminal Code as well. There should be certain codes—security codes, codes of conduct—which people are required to conform to if they have a computer system with respect to different areas of society or different uses of the computer system. If they do not comply with it, then you may get into the unauthorized access question. In other words, it must be important enough for you to try to protect it before you can start charging someone—if you do not use these reasonable security measures. I definitely think your question on security was something that should be looked into.

About a code of ethics, I think you may run into some problems. The United States is looking into this question as well.

Are you talking about a code of ethics for computer programmers and that kind of thing?

Mr. Robinson (Etobicoke—Lakeshore): Yes; yes, indeed.

Ms Kingston: I think you may run into quite a few problems with that. I do not think the computer professionals have any—right now they do not have any standard they have to comply with. They do not have to have gone to university. They do not have to have passed certain courses. Anybody can become a computer programmer, as long as you have the time to learn how to write code. Whether or not they should I think would depend on the section of society they were writing their programs for, or the section of society they were doing electrical engineering for, or whatever their computer expertise has to be.

I think it would depend on the purpose for which they are plying their trade. An internal computer programmer, for example, I do not think should have to comply with the same set of standards as a programmer writing code for general consumption, particularly for the banking community, for example. So you may have to get into a very touchy area there.

[Traduction]

Lawyers' Weekly; je ne sais pas si vous lisez une publication aussi banale.

M. Fortier: Oui.

M. Robinson (Etobicoke—Lakeshore): Il s'intitule *Software Insecurities—Computer Programs and the PPSA*... il s'agit de la Loi sur la sécurité des biens personnels. J'aimerais savoir ce que vous en pensez. Si vous êtes au courant, vous aurez peut-être quelque chose à dire.

Auriez-vous aussi quelque chose à dire concernant un code de déontologie pour le domaine de l'informatique et le traitement des données et ce genre de choses? Je vois que M^{me} Kingston opine de la tête et fait de grands sourires.

Mme Kingston: On m'a découpé l'article du journal qui est sur mon bureau mais je ne l'ai pas encore lu, donc je ne peux pas y répondre.

Au sujet de la sécurité en général, étant donné l'étendu de votre mandat, je crois que c'est très certainement une question qui mérite un examen de votre part. Vous pourriez relier cela à la désignation de certaines nouvelles infractions dans le Code criminel. Il devrait y avoir certains codes de sécurité et des codes de déontologie auxquels les utilisateurs d'un système informatique doivent se conformer par rapport à différents secteurs de la société ou différentes utilisations du système informatique. S'ils ne s'y conforment pas, cela pourrait vous mener à cette question de l'accès non autorisé. Autrement dit, compte tenu de l'importance de l'enjeu, il faudra avoir pris des mesures de sécurité raisonnables; il faut avoir essayé de protéger le système si on veut pouvoir porter une accusation. Je crois très fortement que cette question de sécurité mérite un examen.

Au sujet de code de déontologie, je crois que ça risque de soulever certains problèmes. Aux États-Unis, on étudie cette question aussi.

Parlez-vous d'un code de déontologie pour les programmeurs et ce genre de choses?

M. Robinson (Etobicoke—Lakeshore): Oui.

Mme Kingston: Je crois que cela risque de soulever certaines difficultés. À l'heure actuelle, les programmeurs ne sont pas obligés de se conformer à des normes ou à des critères précis. Ils n'ont pas besoin d'un diplôme universitaire. Il suffit d'apprendre comment écrire le code pour devenir programmeur d'un ordinateur. Je crois que l'existence de critères devrait dépendre du secteur dans lequel ils travaillent, qu'il s'agisse dans l'élaboration de codes, d'un travail d'ingénierie électrique ou d'autres domaines spécialisés.

Je crois que cela varierait selon les circonstances de leur travail. Un programmeur d'une entreprise, à mon avis, ne devrait pas être tenu à respecter les mêmes normes qu'un programmeur qui établit un code pour tout un secteur, particulièrement pour les banques, par exemple. Ça risque d'être un domaine très délicat. Vous allez vous heurter à

[Text]

You are going to get great resistance by the computer section. You may want to consider looking into what the United States is doing right now, because they have looked into that question for years.

Mr. MacIntosh: If I may also speak to you very briefly on this, about ethics and your previous question, what often happens when people commit a successful computer crime is they are not punished; on the other hand they are rewarded by their former employer, who wants to find out how they did it so that future penetration into the system can be prevented. Debates at the present time are going on, quite heated debates, between computer people as to whether this is right or whether there should be some requirement to report a crime, and as to whether this all should be embodied in a code of ethics.

Mr. Robinson (Etobicoke—Lakeshore): Thank you very much.

The Chairman: Before we conclude, maybe I could ask one question of Mr. MacIntosh.

When in your draft section you talk about the consent of the owner, in proposed Section 2.(1), why do you use the word "owner", since we know that most of the people who are dealing with computers do not own the computer; they very often are leasing?

Mr. MacIntosh: Well, it is the person who owns the right to use that computer at that particular time. The word "owner" is used in the broader sense of a person who has at that point the ownership of the use.

The Chairman: Okay, thank you. It was just a point of clarification for me.

Mr. Fortier.

M. Fortier: Pourrais-je ajouter un petit commentaire, madame le président?

Le président: Oui.

M. Fortier: J'aurais dû le faire au tout début.

Contrairement à la politique du Barreau canadien ayant trait aux mémoires déposés devant un comité du Parlement, nous n'avons pas la traduction du texte du mémoire. Ceci est dû, encore une fois, à un manque de temps. Cependant, je peux vous assurer, vous et vos collègues, que le mémoire est en voie d'être traduit et, dans les jours qui suivront, il vous sera remis dans la langue de Molière.

• 1735

J'ai omis, également, de vous dire que deux autres membres permanents du Barreau canadien nous accompagnent aujourd'hui. Il s'agit de Me Eugène Oscanella et M. Lorey Miller. Ce dernier est étudiant à la Faculté de droit de l'Université d'Ottawa et il travaille auprès du directeur exécutif de l'Association durant l'été.

Je vous remercie.

Le président: Je vous remercie de votre présence et de votre présentation. Sachant combien cela est difficile pour une organisation comme la vôtre, qui a des membres à travers tout

[Translation]

beaucoup de résistance de la part des spécialistes en informatique. Cela vous intéressera peut-être de considérer ce qu'on fait aux États-Unis qui se penchent sur cette question depuis des années.

M. MacIntosh: Si vous me permettez de répondre très brièvement à votre question, ce qui se passe très souvent quand quelqu'un réussit un crime dans le domaine de l'informatique, c'est qu'au lieu d'être puni, il est récompensé par son ancien employeur qui veut savoir comment cela était fait de façon à empêcher une pénétration semblable du système à l'avenir. C'est actuellement une question très controversée dans les milieux informatiques: Cette pratique devrait-elle être permise ou devrait-il y avoir obligation de signaler l'infraction et tout cela devrait-il être visé par un code de déontologie?

M. Robinson (Etobicoke—Lakeshore): Je vous remercie beaucoup.

Le président: Avant de conclure, j'ai une question à poser à M. MacIntosh.

Quand votre projet d'article parle de l'assentiment du propriétaire, il s'agit du paragraphe 1 de l'article 2, pourquoi employez-vous le terme «propriétaire» quand dans la plupart des cas, les personnes qui se servent d'ordinateurs n'en sont pas les propriétaires mais les louent simplement?

M. MacIntosh: Eh bien, c'est la personne qui possède le droit d'utiliser l'ordinateur à un moment donné. On emploie le mot dans un sens très large, c'est-à-dire une personne qui possède le droit d'utilisation.

Le président: Merci. C'était simplement une précision.

Monsieur Fortier.

Mr. Fortier: May I add a small comment, Madam Chairman?

The Chairman: Yes.

Mr. Fortier: I should have done so at the outset.

Contrary to the policy of the Canadian Bar with respect to briefs presented to a parliamentary committee, we did not have a translation. Once again, this is due to a lack of time. However, I can assure you and your colleagues that the brief is in the process of being translated and that it will be available in French in the next several days.

I also neglected to mention that we were accompanied today by two other permanent members of the Canadian Bar, Mr. Eugene Oscanella and Mr. Lorey Miller who is a student at the law faculty of the University of Ottawa and is working for the executive director of the Association during the summer.

Thank you.

The Chairman: I would like to thank you for coming and making a statement. We realize how difficult it is for an organization such as yours, with members throughout the

[Texte]

le pays, et connaissant votre façon de fonctionner, nous vous sommes très reconnaissants d'avoir préparé ce mémoire. Il nous sera certainement utile dans la préparation de notre rapport qui sera présenté sous peu. Nous comptons également sur vos réflexions futures en vue d'un projet de loi qui sera soumis, je l'espère, dans un avenir rapproché.

Je vous remercie d'être venus nous rencontrer.

Je désire vous aviser que le Comité siègera demain

... at 10.00 a.m. instead of 9.30 a.m. Mr. Kenneth Chasse lost his father yesterday and will not be able to appear. Instead, we will meet in this room at 10 o'clock with Mr. Stephen Georgas and officials of the Department of Justice. The meeting is adjourned.

[Traduction]

country, especially in view of the procedure you follow, and we are grateful to you for preparing this brief. It will certainly be of use to us in the preparation of our report which will be tabled shortly. We are also counting on your future reflections with respect to a bill which will be submitted, I hope, in the near future.

I would like to thank you for appearing before the committee.

I would like to inform the committee members that the committee will be sitting tomorrow

... à 10h00 au lieu de 9h30. M. Kenneth Chasse a perdu son père hier et ne pourra pas comparaître. Nous allons plutôt nous réunir dans cette salle à 10h00 avec M. Stephen Georgas et les fonctionnaires du ministère de la Justice. La séance est levée.

APPENDIX "COMP-4"

Submission to the Subcommittee on Computer Crime
of the Standing Committee

on

Justice and Legal Affairs

By the

Law, Science and Technology

Committee of the Canadian Bar Association

June 8, 1983

MEMBERS OF THE CANADIAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW, SCIENCE AND TECHNOLOGY

Robin J. Wigdor	- Uxbridge
George Copley	- Victoria
Robert M. Dick	- Prince George
George E. Fisk	- Ottawa
Derek Guthrie	- Montreal
Philip Palmer	- Ottawa
Edward C. Hicks	- Amherst
Joe Schmidt	- Montreal
Judith Kingston	- Toronto
Charles MacIntosh, Q.C.	- Halifax
Grant Murray	- Toronto
Ron Odynski	- Edmonton

This brief was prepared by:

Charles W. MacIntosh, Q.C.	- Halifax
Judith Kingston	- Toronto

The advent of computer technology has brought in its wake many changes. These changes have caused concern in some sections of society that computer technology is creating or could create an exposure to those areas in which it is used, which exposure should be protected by criminal sanctions. On December 16, 1982, Bill C-667 (the "Bill"), entitled "An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime" was introduced by The Honourable Perrin Beatty, P.C., M.P. and given first reading by The House of Commons of Canada.

The paper will address the concerns raised by The Honourable Perrin Beatty in the Bill and then will discuss how such concerns could be met by an alternate solution.

I. BILL C-667: CONCERNS

The explanatory notes in the Bill state that:

"(t)he purpose of this Bill is to address those issues related to computer use and abuse that have traditionally prevented the courts from adequately coming to grips with computer related crime."

However, none of the provisions of the Bill directly face the issue raised in the case of R. v. McLaughlin (1980), 18 C.R. (3d) 399, 53 C.C.C. (2d) 417 (S.C.C.) with respect to use of a computer system as opposed to a telecommunication facility. While the recommended sections 3 and 5 of the Bill might indirectly cover such concerns, a provision either directly setting out an offence

of use of a computer service or including computer time in the definition of section 2 of the Bill might provide more clarity.

Section 1 of the Bill provides a definition of a "computer" which is as follows:

"'computer' means any programmable device or apparatus designed to store or process data or information, but does not include a hand-held calculator or similar device."

It is suggested that this definition may encompass more than what may have been intended. As presently drafted, there are many devices, such as player pianos, which could be caught by this definition. A concern in defining a computer is that it could either be defined in such narrow terms that it does not include future developments in computer technology or be defined so broadly with exclusionary exceptions that such exceptions will not include all the present or future developments in computer technology that should be excluded from a broad definition of a computer. The definition of "computer" in the Bill appears not to be used directly but rather would have an indirect use in defining the words "computer software", "computer data" and "computerized data" as they are used in the Bill. Due to the confusion that may arise by such definition, it may be preferable to omit the definition of a "computer" from the Bill.

Section 2 of the Bill proposes to expand the definition of "property" in section 2 of the Criminal Code R.S.C. (1970), c. C-34, as amended, to include:

"computer software or programs, copies thereof, and retrievable computer data or information produced and stored in machine-readable form by any means".

It is suggested that the use of the words "computer software or programs, copies thereof," may not include certain existing technology such as firmware. The term firmware is sometimes used to refer to instructions contained in read only memory which work with the operating system to control a computer system. It is also unclear why a distinction has been made between computer software and programs, as such distinction could possibly lead to later confusion in the courts. Finally, the use of the words "copies thereof" may not include a copy of computer software or programs which has been made from one medium into a different medium, such as a copy from a listing on paper into a copy on magnetic media. It is further suggested that the words "and retrievable computer data or information produced and stored in machine-readable form by any means" could also lead to confusion. Not only is it unclear why a distinction has been made between retrievable computer data or information, it is also unclear why the word "retrievable" has been included in such definition. If the data or information is not retrievable it would seem rather difficult to retrieve it in order to commit a criminal offence. Finally, the words "produced and stored in machine-readable form by any means" may encompass more than what may have been intended and lead to later confusion in the courts. It could be argued that such words are broad enough to include present computer technology such as the ability to receive voice transmission or

it could be argued that such words are so narrow to include only such data or information that is directly keyed into and stored in a computer system and would not include data or information that was produced originally on a form other than a machine-readable form.

Section 3 of the Bill proposes to create a new section with respect to the criminal offence of theft. It is not clear why section 3 refers to "all or part of a computer program or copy thereof or any computerized data" and excludes the other relevant items in the definition of property as set forth in section 2 of the Bill. Nor is it clear why a distinction has been made between computer data and computerized data. Finally, the use of the word "diverts" in section 3 of the Bill raises some concerns. Not only is it unclear what the meaning of "diverts" is, but it would also be recommended that a section similar to subsection 301.1(2) in the Criminal Code be incorporated in the Bill and refer to both sections 3 and 5 of the Bill. It is suggested that, for consistency and to avoid later confusion, the applicable part of the definition of property in section 2 of the Bill referring to "computer software or programs, copies thereof, and retrievable computer data or information produced and stored in machine-readable form by any means" be included in section 3 of the Bill.

Section 4 of the Bill proposes to expand the definition of property in section 385 of the Criminal Code to include "any computer software or program, or copy thereof, and any retrievable

computer data or information produced and stored in machine-readable form by any means." The comments raised herein with respect to section 2 of the Bill would apply equally to section 4 of the Bill.

Section 5 of the Bill proposes to expand the offence of mischief as described in section 387 of the Criminal Code. The terminology in section 5 wherein subsection 387(c) of the Criminal Code is referred to, include the words "computer program or computer data" rather than the definition of property as set forth in section 4 of the Bill. The applicable comments raised herein with respect to section 3 of the Bill would apply equally to section 5 of the Bill. As well, the use of the word "renders" may cause confusion as it could refer only to computer programs or computer data which has become useless or inoperative or its commercial or scientific value has diminished at the time of destruction or damage rather than allowing for a time period between such events. An example of such occurrence could be a time bomb programmed into computer instructions which is to take effect at some later period of time. Finally, the words "diminishes its commercial or scientific value" may not include computer programs or computer data which are used for personal enjoyment or are not created for purposes of profit or scientific purposes. It is recommended that the use of the words "diminishes its commercial or scientific value" in section 5 of the Bill be clarified.

II. COMPUTER AND CRIME: ALTERNATE SOLUTIONS

1. The Definition of a "Computer"

Legislation dealing with computer abuse must first proceed from an adequate definition of the word "computer" so as to prescribe the limits of the application of the provision and to clearly set forth the matters protected.

What is commonly regarded as a "computer" - a machine to store important information and to perform significant processes - now shares many functions with lesser apparatus such as hand calculators, video games and automotive ignition systems.

To define the "computer" which the law should seek to protect is becoming increasingly difficult as new uses of electronic technology come on the market.

Definitions of the word "computer" contained in existing or proposed legislation have been criticized for being too narrow in scope or too broad.

ARIZONA

"Computer" means an electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

This definition, similar to that found in the Federal Computer Systems Protection Act of 1979, has been criticized as being too narrow in that it is limited to electronic devices that manipulate data via electronic or magnetic impulses, excluding some major new forms of computers, such as those that employ fluidics. It has also been criticized for not limiting its scope to general purpose machines, opening the way for rulings that electronic watches and other automated devices are covered by the legislation.¹

¹Gemignani, Law and the Computer, CBI Publishing Company, Inc., Mass. p.144

FLORIDA

"Computer" means an internally programmed, automatic device that performs data processing.

This definition avoids the electronic restriction of the Arizona statute, but does not limit the word to general purpose machines, thus including such things as highway traffic signal systems.

MODEL COMPUTER CRIME BILL

"Computer" means an internally programmed, general purpose, automatic device that performs data processing.

This definition resolves most of the problems found in earlier definitions, but it depends upon an interpretation of the phrase 'data processing'.

ILLINOIS

"Computer" means an internally programmed, general purpose digital device capable of automatically accepting data, processing data and supplying the results of the operation.

This definition appears to have none of the problems encountered in the foregoing definitions but restricts the word to 'digital', thus excluding analog computers.

RECOMMENDATION

We recommend the Illinois definition with deletion of the word 'digital'.

"Computer" means an internally programmed, general purpose device capable of automatically accepting data, processing data and supplying the results of the operation.

2. Protection of Extended System

Computers are rarely found in isolation, but are usually connected to a variety of other equipment. Interference with peripheral equipment may preclude the owner from using his computer or otherwise interfere with normal operation.

It is submitted that protection is needed for the extended system as well as for the computer itself.

"Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

3. Protection of Software

It is the software in the computer that makes it perform a specific task. Software may also comprise written programs and data.

If a written program is fraudulently altered and then introduced into the computer it may be more damaging an event than dishonest alteration of data already resident in the machine.

It is submitted that protection should be afforded to a computer program in written form as well as one in a computer.

Michigan makes it an offence to alter or destroy a computer, computer system or computer network and makes use of three interconnected definitions.

"Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

"Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

"Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

4. The Description of the Offence

It has been suggested that the Mischief section of the Criminal Code might be suitably modified so as to cover computer crime.

It is submitted that computer crime can have costly and far-reaching consequences that make such an approach inappropriate.

The Mischief section is associated in the mind of the public with such pranks as spraying paint on statues, breaking school fixtures and damaging car radio aerials.

Computer crime can result in the theft of millions of dollars and even endanger human life, as for instance when a hospital computer with patient records is put out of commission or an aircraft guidance system is altered. Many computer criminals are, indeed, unaware of the ultimate consequences of their acts since they do not always know the varied uses to which a particular computer system is being put.

A computer machine may be like other property and superficial damage to a panel of the processing unit can be classified as mischief, but wilful destruction of data or a major system component may have far-reaching consequences and should, it is submitted, be regarded as a separate substantive offence.

5. Types of Computer Abuse

The various degrees of computer abuse have been very clearly distinguished in a Brief to the National Consultation on Computer Crime, Department of Justice, Canadian Information Processing Society, Toronto, March 2 & 3, 1983 by Frank Spitzer, Faculty Liaison Officer of the University of Toronto Computing Services.

"Most 'computer crime' falls into one of the following categories:

- a. Theft of time,
- b. theft of information,
- c. modification of data,
- d. interference with the operation of the system,
- e. interference with the use, by an individual, of a computer system, or
- f. the use of the computer as an instrument in the perpetrating of a criminal offence, e.g. code breaking.

"Each of the subdivisions just noted, represents in reality problems which have long existed, but when they existed without the use of a computer, the problems were not regarded in the same light. Either existing laws were bent in order to satisfy the problem, or alternatively, in many cases, the problems were small enough that they were dealt with in an otherwise satisfactory matter. The recent explosive growth of the computer environment where the scale and scope of problems has become immense, has focused on the inadequacy both of the mechanisms

for detection and on the mechanisms for prevention of these activities.

- A. Theft of Time - Returning to the list of computer aided involvements, the theft of time should be explained. Typically, it means the use of a computer and its cycles without the knowledge or authorization of its owner. Typically, there will be no cost to the owner other than some displaced usage for which they might otherwise have charged. It might be argued that in the straight theft of time situation, proprietary programs may be used which would otherwise incur some costs due to royalties.

Some extra maintenance or back-up procedures may also be involved if this use is extensive. A careful check however, shows that almost every computer system runs with substantial idle time which would not lead to any loss of money. The use of proprietary programs is often covered under various contractual arrangements and these would however, be circumvented by such use.

- B. Theft of Information - The theft of information is clearly a far more delicate situation and would normally include the theft of trade secrets, financial information and the like. This material could, in a traditional office sense, often have been acquired by the use of a photocopying machine and access to an appropriate filing cabinet. Industrial espionage would then have been a possible term. Again this theft is undetectable since nothing has been taken, nothing has been touched, and the real owner of the information has no mechanism for knowing that it has occurred. No cost in any real sense is incurred by the owner, nor by the operator of the computer, except for the potential loss of business which may accrue from the loss of this confidential information. In some cases, for example a mailing list, the inability to subsequently sell the mailing list or sell the computer program as a result of its already having been sold or placed in the public domain, may be a very real loss in the longer run.

- C. Modification of Data - The existance of large databanks maintained by companies now capable of mailing to a very specifically targeted audience may be the result of an invasion of privacy by a large number of agencies. These agencies have included banks and governments who make limited segments of their data available believing that it will not infringe people's privacy. The use, for example, of social insurance numbers by many organizations as a key to their employees and the subsequent selling of certain extracts of their employee database to such mailing agencies is no different than the kinds of things which were previously done by these companies as good corporate citizens. Multiple sales organizations now cull this information in such a manner that it is put together in a highly refined form. An example in the university context exists in the form of a research project undertaken by a group of dentists following the growth and ageing of a large body of population over a period of years. This information has been "borrowed" quite legally and openly by a number of similar research institutions throughout the world. The University of Toronto research team has grave concerns that this information may surface under the guise of having originated elsewhere, since they have by now distributed the equivalent of the entire database in multiple sections. Their ability to police and protect the originality, the confidentiality and the authenticity of their work leaves them concerned. They certainly have no evidence, but it is also conceivable that this data could have been stolen in total without their knowledge. They would then lose the opportunity to pursue research grants to further support their world renowned work.
- D. Interference with Operation of the System - Some illicit access to computers is aimed at taking control of the computer system. This clearly involves considerable annoyance, embarrassment and potentially, loss of business revenue to the organization concerned. An extreme instance has been documented whereby a computer system was penetrated by knowledgeable people and so modified that after it had ceased to function,

it took experts a number of days to bring the system back into normal operation. Clearly, if the computer involved is concerned either with critical business, national security or the functioning of a large organization, the loss of productivity because of many people incapable of performing their daily tasks represents a considerable financial burden to anybody involved.

- E. Interference with the Use by an Individual of a Computer System - On other occasions, the same technique may be aimed at a single individual who finds his files tampered with, his account modified (eg. his password changed), or merely his results garbled.
- F. Use of the Computer as an Instrument in the Perpetrating of a Criminal Offence - In many cases, organizations go to considerable lengths to protect their data through the use of encryption, algorithms, or other sophisticated techniques. The use of the computer to break these safeguards is an obvious and almost proper use of these machines. Certainly governments do exactly this when tapping communications lines, and yet the use of computers in this form certainly has nothing identified in the Criminal Code until the results are used successfully in the pursuit of conventional crime."

6. Penalty

Computer crime ranges from the serious to the ridiculous - from acts threatening lives and enormous economic consequences to trivial pranks. For this reason, the authorities should have the option to lay a charge as either an indictable offence or a summary conviction offence.

7. Suggested Legislation

It is submitted that the following section incorporates the foregoing suggestions in a manner that would achieve the intended purposes.

SUGGESTED DRAFT SECTION

394A(1) In this Section

*as used
does
not mean*

"Computer" means an internally programmed, general purpose device capable of automatically accepting data, processing data and supplying the results of the operation.

"Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

"Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

"Computer system" means a set of related, connected or unconnected, computer equipment, devices, and includes computer software.

(2) Everyone who, without lawful excuse,

(2.1) obtains the use of a computer system or any part thereof, without the consent of the owner, or

(2.2) alters or destroys computer programs or computer software without the consent of the owner

is guilty of

(a) an indictable offence and is liable to imprisonment for ten years; or

(b) an offence punishable on summary conviction.

APPENDICE «COMP - 4»

Mémoire au Sous-comité sur les infractions relatives aux ordinateurs
du Comité permanent

de la

justice et des questions juridiques

Comité du droit, de la science et de la technologie
de l'Association du barreau canadien

Le 8 juin 1983

MEMBRES DU COMITE PERMANENT
DU DROIT, DE LA SCIENCE ET DE LA TECHNOLOGIE
DE L'ASSOCIATION DU BARREAU CANADIEN

Robin J. Wigdor	- Uxbridge
Diane O. Campbell	- Summerside
Robert M. Dick	- Prince-George
Ron Gravelle	- Ottawa
Derek Guthrie	- Montréal
Michael Hetu	- Ottawa
Edward C. Hicks	- Amherst
Ian L. Jessiman	- Victoria
Judith Kingston	- Toronto
Charles MacIntosh c.r.	- Halifax
Grant Murray	- Toronto
Ron Odynski	- Edmonton

Le présent mémoire a été préparé par:

Charles W. MacIntosh c.r.	- Halifax
Judith Kingston	- Toronto

L'avènement de l'informatique a apporté dans son sillage, de nombreux changements, qui ont fait craindre à certains que cette nouvelle technique n'entraîne, dans les divers secteurs où elle est utilisée, des risques dont il faudrait se prémunir dans le code pénal. Le 16 décembre 1982, l'honorable Perrin Beatty, C.P., député, déposait donc à la Chambre des communes, pour première lecture, le projet de loi C-667 (le «projet de loi»), intitulé «Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs».

Dans le présent document, nous nous pencherons sur les grandes questions soulevées par l'honorable Perrin Beatty dans ce projet de loi et discuterons ensuite des autres solutions possibles au problème de la criminalité informatique.

1. PROJET DE LOI C-667: GRANDES QUESTIONS

Les notes explicatives contenues dans le projet de loi comprennent l'extrait suivant:

«Ce projet de loi vise à résoudre certains problèmes entourant l'emploi des ordinateurs qui traditionnellement ont empêché les tribunaux de s'attaquer convenablement au crime dans le domaine des ordinateurs.»

Cependant, aucune des dispositions du projet de loi ne s'attaque directement à la question soulevée dans l'affaire R. C. McLaughlin (1980), 18 C.R. (3d) 399, 53 C.C.C. (2d) 417 (S.C.C.) en ce qui a trait à l'utilisation d'un système informatique, par opposition à un service de télécommunication. Bien que les articles 3 et 5 du projet de loi couvrent indirectement ces aspects, il serait plus clair d'ajouter au texte une disposition prévoyant expressément que l'utilisation frauduleuse d'un service informatique constitue une infraction, ou d'inclure la notion de temps-machine dans la définition donnée à l'article 2 du projet de loi.

Le terme «ordinateur» est défini de la façon suivante à l'article 1 du projet de loi:

««ordinateur» désigne tout appareil ou dispositif informatisé destiné à emmagasiner ou traiter de l'information, à l'exclusion d'un calculateur ou autre petit appareil ou dispositif semblable.»

Cette définition est en fait plus générale que ce que semblent avoir prévu les législateurs. Telle quelle, elle pourrait en effet englober de nombreux appareils, par exemple les pianos mécaniques. Le problème que pose la définition du terme «ordinateur», c'est que si celle-ci est trop restrictive,

elle exclut tout perfectionnement futur dans le domaine de l'informatique, et si elle est trop vague et comporte trop d'exceptions, ces dernières ne peuvent tenir compte de tous les perfectionnements actuels ou futurs qui devraient être exclus d'une définition générale de l'ordinateur. La définition que comprend le projet de loi ne semble pas destinée à être appliquée directement, mais plutôt à permettre de définir indirectement les définitions «logiciel d'ordinateur», «information entrée sous une forme repérable par ordinateur» et «information mise en oeuvre sur ordinateur», utilisées dans le projet de loi. Étant donné la confusion qu'elle risque d'entraîner, il serait peut-être préférable de la supprimer purement et simplement.

A l'article 2 du projet de loi, on propose d'étendre la définition des termes «biens» ou «propriété», donnée à l'article 2 du Code criminel, S.R.C. (1970) c. C-34, tel que modifié, pour inclure:

«les logiciels ou programmes d'ordinateur, les copies de logiciels ou programmes d'ordinateur, et l'information entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisée».

Or, nous estimons que l'utilisation des mots «les logiciels ou programmes d'ordinateur, les copies de logiciels ou programmes d'ordinateur» risquent d'exclure certaines techniques existantes comme la microprogrammation. (Ce terme est quelque-fois employé pour désigner les instructions contenues dans la mémoire morte et qui se combinent au système d'exploitation pour régler le fonctionnement du système informatique.) Il est par ailleurs difficile de comprendre pourquoi les législateurs ont fait, entre les logiciels et les programmes d'ordinateur, une distinction qui risque, plus tard, d'être cause de confusion devant les tribunaux. Enfin, l'utilisation des mots «les copies de logiciels ou programmes d'ordinateur» n'incluent pas nécessairement les changements de support, par exemple si une liste sur papier est transférée sur support magnétique. Nous estimons par ailleurs que les mots «et l'information entrée sur une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé» pourraient également prêter à confusion. Tout d'abord, la version anglaise établit une distinction difficilement justifiable entre les termes «data» et «information». Ensuite, on peut se demander pourquoi l'expression «repérable par ordinateur» a été incluse dans cette définition; en effet, si l'information n'est pas repérable par ordinateur, il semble assez difficile de l'extraire pour commettre un acte criminel. Enfin, les mots «emmagasinée sur un enregistrement informatisé» peuvent être interprétés de façon plus générale que ce qu'avaient voulu les législateurs et prêter à confusion devant les tribunaux. Certains pourraient en effet soutenir que ces mots sont assez généraux pour inclure diverses techniques informatiques nouvelles comme l'aptitude à assimiler des instructions orales, alors que d'autres pourraient en donner une interprétation restreinte, estimant qu'ils n'englobent que l'information directement introduite par clavier et stockée dans un système informatique, à l'exclusion de

l'information produite à l'origine sous une forme non repérable par ordinateur.

L'article 3 du projet de loi est destiné à inclure dans le Code criminel un nouvel article sur le vol. On peut se demander pourquoi il est question à l'article 3 de «tout ou partie d'un logiciel, ou copie de logiciel, ou toute information mise en oeuvre sur ordinateur», et non des autres éléments inclus dans la définition du terme «biens» à l'article 2 du projet de loi. On peut également s'interroger sur la raison pour laquelle les auteurs ont cru bon d'établir une distinction entre l'«information entrée sous une forme repérable par ordinateur» et l'«information mise en oeuvre sur ordinateur». Enfin, l'utilisation du mot «détourne», à l'article 3 du projet de loi, pose certains problèmes. Non seulement ce terme est ambigu, mais en outre, il serait bon d'inclure dans le projet de loi un article semblable au paragraphe 301.1(2) du Code criminel, qui se rattacherait à la fois aux articles 3 et 5 du projet de loi. Afin d'assurer l'uniformité et d'éviter toute confusion ultérieure, nous recommandons que la partie applicable de la définition du terme «biens», à l'article 2 du projet de loi, à savoir «les logiciels ou programmes d'ordinateur, les copies de logiciels ou programmes d'ordinateur, et l'information entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé», soit incluse dans l'article 3 du projet de loi.

À l'article 4, les législateurs proposent d'étendre la définition du terme «bien», à l'article 385 du Code criminel, pour y inclure les mots suivants: «tout logiciel ou programme d'ordinateur, ou copie de logiciel ou de programme d'ordinateur, et toute information entrée sous une forme repérable par ordinateur et emmagasinée sur un enregistrement informatisé». Les commentaires que nous venons de faire au sujet de l'article 2 du projet de loi s'appliquent également à l'article 4.

À l'article 5, on propose d'étendre la définition que l'article 387 du Code criminel donne du terme «méfait». Dans la citation renvoyant au paragraphe 387(1)c) du Code criminel, on emploie les mots «un logiciel d'ordinateur ou de l'information mise sur ordinateur», plutôt que la définition du terme «bien» qui se trouve à l'article 4 du projet de loi. Nos observations au sujet de l'article 3 du projet de loi s'appliquent donc également à l'article 5. En outre, le terme «deviennent» peut prêter à confusion, parce qu'il pourrait ne désigner que les programmes ou les données qui sont devenus inutiles ou inopérants, ou dont la valeur commerciale ou scientifique a diminué, au moment même du méfait, et non plus tard, sans tenir compte de la possibilité qu'une «bombe à retardement» soit programmée dans un ordinateur. Enfin, les mots «leur valeur commerciale ou scientifique est diminuée» semblent exclure les données ou les logiciels utilisés dans des jeux, ou créés pour des fins autres que commerciales ou scientifiques. Nous recommandons par conséquent de trouver une formule plus claire que «leur valeur commerciale ou scientifique est diminuée» pour l'article 5 du projet de loi.

II. AUTRES SOLUTIONS AU PROBLEME DE LA CRIMINALITE INFORMATIQUE

1. La définition du terme «ordinateur»

La législation sur la criminalité informatique doit d'abord se fonder sur une définition exacte du terme «ordinateur», afin de prescrire les limites d'application des dispositions adoptées et de décrire clairement les éléments protégés.

L'appareil qu'on appelle communément «ordinateur», c'est-à-dire celui qui sert à stocker de l'information importante et à remplir des fonctions diverses, partage maintenant bon nombre de ces fonctions avec des appareils moins importants comme les calculatrices de poche, les jeux vidéo et les systèmes d'allumage des véhicules automobiles.

Il est donc de plus en plus difficile de définir en quoi consiste l'«ordinateur» que la loi doit tenter de protéger, au fur et à mesure que les nouvelles techniques électroniques se répandent sur le marché.

La plupart des lois actuelles ou proposées ont été critiquées pour leur définition trop restrictive ou trop générale du terme «ordinateur».

ARIZONA

Le terme «ordinateur» désigne un appareil électronique qui exécute des fonctions de logique, d'arithmétique ou de mémorisation par la manipulation d'impulsions électroniques ou magnétiques; il comprend tous les instruments d'entrée, de sortie, de traitement, de stockage et de communication, ainsi que les logiciels, qui sont reliés à cet appareil dans un système ou un réseau.

Cette définition, semblable à celle qui se trouve dans la Federal Computer Systems Protection Act de 1979, a été critiquée pour son caractère restrictif, en ce sens qu'elle est limitée aux appareils électroniques permettant de manipuler des données au moyen d'impulsions électroniques ou magnétiques, ce qui exclut d'importantes catégories nouvelles d'ordinateurs, comme ceux qui emploient la fluidique. Par ailleurs, cette définition n'est pas limitée aux appareils polyvalents, ce qui ouvre la voie à des décisions judiciaires selon lesquelles les montres électroniques et divers autres appareils automatiques seraient couverts par cette loi--(1).

1. Gemignani, Law and the Computer, CBI Publishing Company, Inc., Mass., p.144.

FLORIDE

Le terme «ordinateur» désigne un appareil automatique programmé qui exécute le traitement de données.

Cette définition évite de restreindre le terme aux appareils électroniques comme le fait la loi de l'Arizona, mais ne le limite pas aux appareils polyvalents; elle pourrait donc englober divers appareils comme les systèmes de signalisation routière.

PROJET DE LOI MODÈLE SUR LA CRIMINALITÉ INFORMATIQUE

Le terme «ordinateur» désigne un appareil automatique programmé polyvalent qui exécute le traitement de données.

Cette définition résout la plupart des problèmes que posent les autres définitions, mais tout dépend alors de l'interprétation de l'expression «traitement de données».

ILLINOIS

Le terme «ordinateur» signifie un appareil à fonctionnement numérique polyvalent programmé de l'intérieur et capable automatiquement d'accepter des données, de les traiter et de fournir les résultats de l'opération.

Cette définition ne semble poser aucun des problèmes que soulèvent les autres, mais limite ce terme aux appareils «à fonctionnement numérique», ce qui exclut les ordinateurs analogiques.

RECOMMANDATION

Nous recommandons par conséquent d'adopter la définition de l'Illinois, en supprimant l'expression «à fonctionnement numérique».

Le terme «ordinateur» signifie un appareil polyvalent programmé de l'intérieur et capable automatiquement d'accepter des données, de les traiter et de fournir les résultats de l'opération.

2. Protection de l'ensemble d'un système

Les ordinateurs se retrouvent rarement seuls; ils sont habituellement reliés à toute une gamme d'autres appareils. En nuisant au fonctionnement de l'équipement périphérique, il est possible de gêner le

fonctionnement normal de l'ordinateur, ou même d'empêcher son propriétaire de s'en servir.

Nous estimons donc qu'il faut protéger l'ensemble du système, tout comme l'ordinateur lui-même.

«Réseau informatique» signifie l'interconnexion de lignes de communication avec un ordinateur par le biais de terminaux, ou un complexe composé de deux ordinateurs interconnectés ou plus.

3. Protection du logiciel

C'est le logiciel qui fait effectuer à un ordinateur une tâche spécifique. Le logiciel peut également comprendre des programmes et des données écrits.

L'introduction dans un ordinateur d'un programme écrit frauduleusement modifié peut avoir des conséquences plus graves que la modification malhonnête de données déjà stockées dans un ordinateur.

Selon nous, il faut protéger les programmes informatiques sous leur forme écrite, ainsi qu'une fois chargés dans l'ordinateur.

Au Michigan, commet une infraction quiconque modifie ou détruit un ordinateur, un système ou un réseau informatiques. La législation du Michigan utilise les trois définitions suivantes:

«Programme informatique» signifie une suite d'instructions assimilables par l'ordinateur, qui permet le fonctionnement d'un système informatique d'une façon conçue pour obtenir les résultats appropriés.

«Logiciel informatique» signifie un ensemble de programmes et de procédures informatiques et de documents connexes portant sur le fonctionnement d'un système informatique.

«Système informatique» signifie un ensemble de machines et de mécanismes informatiques, connectés ou non, ainsi que le logiciel informatique.

4. Description de l'infraction

Certains ont proposé que l'article du Code criminel portant sur les méfaits soit modifié de façon à englober les délits informatiques.

Nous soutenons pour notre part que les délits informatiques, pouvant avoir des conséquences coûteuses et aux retombées considérables, cette méthode ne convient pas.

Dans l'esprit du public, l'article sur les méfaits évoque des actes de vandalisme comme peindre des statues, casser du matériel scolaire et endommager des antennes d'automobile.

En revanche, la criminalité informatique peut entraîner le vol de millions de dollars et même mettre en danger des vies humaines comme dans le cas où un ordinateur d'hôpital contenant les dossiers des malades est rendu inutilisable ou celui où un système de guidage d'avions est modifié. De nombreux auteurs de délits informatiques ignorent en fait les conséquences finales de leurs actes étant donné qu'ils ne connaissent pas toujours les diverses utilisations d'un système informatique.

Un ordinateur est un bien au même titre que d'autres et des dommages superficiels à un panneau d'une unité centrale peuvent être classés comme un méfait. En revanche, la destruction délibérée de données ou d'un élément important du système peut avoir des conséquences énormes et doit, selon nous, être considérée comme un délit important distinct.

5. Genres de délits informatiques

La distinction entre les divers degrés de délits informatiques a été très clairement exposée dans un mémoire présenté par Frank Spitzer, responsable des rapports avec les enseignants du Service informatique de l'Université de Toronto au cours de la Consultation nationale sur la criminalité informatique organisée par le ministère de la Justice et l'Association canadienne de l'informatique à Toronto, les 2 et 3 mars 1983.

«La plupart des «délits informatiques» appartiennent à l'une des catégories suivantes:

- a. Vol de temps-machine
- b. vol d'informations
- c. modification de données
- d. obstacle au bon fonctionnement d'un système
- e. obstacle à l'utilisation d'un système informatique par une personne, ou
- f. utilisation de l'ordinateur pour perpétrer un délit, par exemple, le décryptage d'un code.

Toutes ces catégories représentent en fait des problèmes qui existent depuis longtemps, mais avant l'avènement de l'ordinateur on ne les considérait pas du même oeil. On étirait un peu la portée de la loi pour résoudre le problème ou bien, dans de nombreux cas, les problèmes étaient assez peu importants pour qu'on puisse les régler d'une autre façon satisfaisante. La récente «explosion informatique» a accru considérablement la portée et l'ampleur des problèmes et a donc ressortir les lacunes des mesures de détection et de prévention de la criminalité. Les problèmes juridiques ont

perdu de leur priorité à cause du faible taux d'inculpations. Le présent document a pour objet de faire ressortir l'absolue nécessité d'adopter des mesures de protection d'ordre juridique: adéquates pour assurer que les personnes arrêtées paieront un juste prix pour leurs agissements.

- A. Vol de temps-machine - Pour en revenir à la liste des catégories de délits informatiques, il convient d'expliquer la notion de vol de temps-machine. En règle générale, le vol de temps-machine signifie l'utilisation d'un ordinateur et de ses cycles à l'insu ou sans l'autorisation de son propriétaire. Ce genre de vol ne coûte en fait rien au propriétaire si ce n'est la somme qui aurait autrement été facturée à un utilisateur légitime. On pourrait soutenir que dans les cas de vol de temps-machine simples, les délinquants utilisent parfois des programmes déposés pour lesquels on facturerait normalement des redevances.

Si ces programmes sont beaucoup utilisés, cela peut entraîner des frais additionnels au chapitre de la maintenance ou des procédures de secours. Néanmoins une vérification soigneuse démontre que presque tous les systèmes informatiques sont oisifs une bonne partie du temps, ce qui n'entraîne aucune perte d'argent. Cependant, l'utilisation de programme déposés est souvent couverte par divers contrats et toute utilisation non autorisée entraîne par conséquent des pertes.

- B. Vol d'informations - Le vol d'informations est une question évidemment beaucoup plus délicate et il engloberait normalement le vol de secrets industriels, ou de renseignements financiers ou d'autres données du même genre. Dans un bureau classique, ces informations auraient été photocopiées par une personne ayant accès au classeur approprié. On aurait pu alors parler d'espionnage industriel. Une fois encore, ce genre de vol est impossible à déceler, étant donné que rien n'est pris, rien n'est touché, et que le véritable propriétaire de l'information n'a aucun moyen de savoir ce qui s'est passé. Ce genre de vol n'entraîne aucun coût réel, ni pour le propriétaire, ni pour l'opérateur de l'ordinateur, exception faite de la perte financière éventuelle qui peut résulter du vol de renseignements confidentiels. Dans certains cas, par exemple dans celui d'une liste d'adresses, l'impossibilité de vendre par la suite cette liste ou le programme informatique correspondant parce qu'ils ont déjà été vendus ou rendus publics peut entraîner à long terme une perte très réelle.
- C. Modification de données - L'existence de vastes banques de données entretenues par des sociétés maintenant capables

d'envoyer des documents à un public choisi en fonction de critères extrêmement précis peut résulter de l'invasion de la vie privée par un grand nombre d'organismes. Ces organismes font appel aux banques et aux administrations publiques qui divulgent des éléments limités de leurs données, persuadés qu'ils ne violent en rien ainsi la vie privée des intéressés. Par exemple, l'utilisation de numéros d'assurance-sociale par de nombreuses entreprises pour classer les données sur leurs employés et la vente, par la suite, de certaines parties de ces données à des organismes de distribution postale ne diffèrent en rien de ce que faisaient autrefois ces sociétés en toute bonne foi. Les organisations de vente multiple rassemblent maintenant ces informations d'une manière très perfectionnée. On peut citer à titre d'exemple dans le milieu universitaire un programme de recherche exécuté par un groupe de dentistes suivant de près pendant un certain nombre d'années la croissance et le vieillissement d'un vaste segment de la population. Les données ainsi recueillies ont été «empruntées» très légalement et ouvertement par un certain nombre d'institutions de recherches analogues du monde entier. L'équipe de recherche de l'Université de Toronto est très préoccupée par le fait que ces renseignements pourraient être diffusés ailleurs en leur prêtant une origine différente, étant donné qu'elle a maintenant distribué l'ensemble de la base de données en multiples sections. L'équipe de recherche se demande avec inquiétude comment contrôler et protéger l'originalité, la confidentialité et l'authenticité de ses travaux. Il n'existe évidemment aucune preuve, mais ces données pourraient aussi avoir été volées à l'insu des chercheurs. Ceux-ci pourraient ainsi se retrouver dans l'impossibilité de solliciter des bourses de recherche pour poursuivre leurs travaux dont la valeur est reconnue dans le monde entier.

- D. Obstacle au bon fonctionnement d'un système - Il arrive aussi que l'on obtienne accès à un ordinateur en vue de prendre le contrôle du système informatique. Cela peut évidemment entraîner des difficultés considérables pour l'organisation visée, ainsi qu'un manque à gagner possible. Un cas extrême de ce genre a déjà été rapporté: des personnes bien informées ont pénétré un système informatique et l'ont modifié de telle sorte qu'une fois qu'il a cessé de fonctionner, il a fallu à des experts plusieurs jours pour en rétablir le fonctionnement normal. De toute évidence, si l'ordinateur dont il s'agit sert à traiter des questions d'une importance financière cruciale, des questions de sécurité nationale ou s'il assure le fonctionnement d'une vaste organisation, la perte de productivité résultant du fait que de nombreuses personnes

sont dans l'impossibilité d'exécuter leurs tâches quotidiennes représente une perte financière considérable.

- E. Obstacle a l'utilisation d'un systeme informatique par une personne - La même technique peut viser une seule personne qui découvre un jour que ses fichiers ont été manipulés, ou que son compte a été modifié (par exemple, son mot de passe changé) ou tout simplement que ses résultats ont été falsifiés.
- F. Utilisation de l'ordinateur pour perpétrer un délit - De nombreux organismes se donnent beaucoup de mal pour protéger leurs données en utilisant des codes, des algorithmes ou d'autres techniques perfectionnées. Or, se servir d'un ordinateur pour passer outre ces précautions est une utilisation évidente et presque appropriée de ces machines. C'est exactement ce que font les gouvernements qui écoutent des lignes de communication. Pourtant, l'utilisation de l'informatique de cette manière n'est pas prévue dans le Code criminel, du moins tant que des résultats ainsi obtenus ne serviront pas à la lutte contre la criminalité classique.

6. Peines

Les délits informatiques sont variés: certains sont très graves et d'autres anodins; certains menacent des vies ou ont des répercussions financières considérables et d'autres ne sont que des blagues sans conséquence. Pour cette raison, les autorités devraient pouvoir accuser les contrevenants soit d'acte criminel, soit d'infraction punissable sur déclaration sommaire de culpabilité, selon le cas.

7. Mesure législative proposée

Selon nous, l'article suivant incorpore les suggestions précitées d'une façon permettant d'atteindre les objectifs visés.

PROJET D'ARTICLE

394A(1) Dans le présent article,

«Ordinateur» signifie une machine automatique polyvalente programmable capable d'accepter des données, de les traiter et de fournir les résultats de l'opération.

«Programme informatique» signifie une suite d'instructions assimilables par un ordinateur, permettant le fonctionnement d'un système informatique d'une façon conçue pour obtenir les résultats appropriés.

«Logiciel informatique» signifie un ensemble de programmes et de procédures informatiques et de documents connexes portant sur le fonctionnement d'un système informatique.

«Système informatique» signifie un ensemble de machines et de mécanismes informatiques, connectés ou non, et comprend le logiciel informatique.

(2) Quiconque, sans apparence de droit,

(2.1) utilise un système informatique ou une partie d'un tel système sans l'autorisation du propriétaire, ou

(2.2) modifie ou détruit des programmes ou du logiciel informatiques sans l'autorisation du propriétaire

est coupable

(a) d'un acte criminel et est passible d'une peine d'emprisonnement de dix ans;

(b) d'une infraction punissable sur déclaration sommaire de culpabilité.



If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESSES—TÉMOINS

From the Canadian Bar Association:

Mr. Yves Fortier, President;
Mr. Bernard E. Blanchard, Executive Director;
Ms. Judith Kingston and
Mr. Charles W. MacIntosh, Q.C., of the Standing Committee on Law, Science and Technology.

De l'Association du Barreau canadien:

Me Yves Fortier, président;
Me Bernard E. Blanchard, directeur-exécutif;
Me Judith Kingston et
Me Charles W. MacIntosh, C.R., du Comité permanent sur le droit, sciences et technologie.

HOUSE OF COMMONS

Issue No. 17

Thursday, June 9, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 17

Le jeudi 9 juin 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Matters pertaining to the Order of Reference

CONCERNANT:

Questions relatives à l'ordre de renvoi

WITNESSES:

(See back cover)

TÉMOINS:

(Voir à l'endos)



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

SUB-COMMITTEE ON COMPUTER CRIME
OF THE STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

Chairman: Mrs. Céline Hervieux-Payette

Vice-Chairman:

SOUS-COMITÉ SUR LES INFRACTIONS
RELATIVES AUX ORDINATEURS DU COMITÉ
PERMANENT DE LA JUSTICE ET DES QUESTIONS
JURIDIQUES

Président: M^{me} Céline Hervieux-Payette

Vice-président:

MEMBERS/MEMBRES

Hon. Ray Hnatyshyn
Claude-André Lachance
Ms. Lynn McDonald (*Broadview—Greenwood*)

DESIGNATED ALTERNATES/SUBSTITUTS
DÉSIGNÉS

Hon. Perrin Beatty
Ken Robinson (*Etobicoke—Lakeshore*)

(Quorum 3)

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

MINUTES OF PROCEEDINGS

THURSDAY, JUNE 9, 1983
(19)

[Text]

The Sub-committee on computer crime met this day at 10:26 o'clock a.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (Etobicoke—Lakeshore).

In attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

Witnesses: Mr. Stephen Georgas, Solicitor, Toronto. *From the Department of Justice:* Mr. E.A. Tollefson, Coordinator, Criminal Code Review; Mr. Norman Hill, Project Chief, Theft and Fraud Project.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

Mr. Georgas made a statement and answered questions.

At 11:25 o'clock a.m., the sitting was suspended.

At 11:31 o'clock a.m., the sitting resumed.

Mr. Tollefson made a statement and, with Mr. Hill, answered questions.

At 12:31 o'clock p.m., the Sub-committee adjourned, to the call of the Chair.

PROCÈS-VERBAL

LE JEUDI 9 JUIN 1983
(19)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à 10h26 sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (Etobicoke—Lakeshore).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Témoins: Me Stephen Georgas, avocat, Toronto. *Du Ministère de la Justice:* M. E.A. Tollefson, coordonnateur, Révision du Code criminel; M. Norman Hill, Chef de projet, Projet vol et fraude.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1*).

M. Georgas fait une déclaration et répond aux questions.

A 11h25, la séance est suspendue.

A 11h31, la séance reprend.

M. Tollefson fait une déclaration et, avec M. Hill, répond aux questions.

A 12h31, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité

Pierre de Champlain

Clerk of the Sub-committee

EVIDENCE

*(Recorded by Electronic Apparatus)**[Texte]*

Thursday, June 9, 1983

• 1026

Le président: À l'ordre!

Le Sous-comité reprend l'étude de son ordre de renvoi concernant les infractions relatives aux ordinateurs.

Ce matin, nous recevons M. Stephen Georgas, avocat de Toronto, ainsi que M. E.A. Tollefson, du ministère de la Justice. Je demande donc à M. Georgas de présenter son exposé.

We welcome him to Ottawa and thank him for appearing before us and helping us in finalizing the study of this important subject-matter.

Mr. Stephen Georgas (Barrister and Solicitor, Toronto): Thank you, Madam Chairman.

The approach I am taking to analysing Bill C-667 is to look at what conduct, what computer-related conduct, I would consider to be criminal, from there to see whether the Criminal Code, as it now is, covers that particular conduct, and then, if not, to what extent the Beatty bill does.

Just as a brief opening remark, it is my opinion that in considering whether conduct is criminal or not we should not assume that the criminal law is a substitute for any shortcomings in other areas of law, such as laws relating to intellectual property rights, or laws relating to trade secrecy, or our civil law. We should be looking at it strictly in relation to whether the conduct itself is criminal.

With that in mind, I have tried to consider which forms of conduct would, from a computer standpoint, be criminal. I break it down into two basic types of conduct: conduct where a computer is used as an instrument of abuse and conduct where a computer is used as an object of abuse.

In the first classification, I would look at fraud-related offences, mischief-related offences, and the broad range of activity that we consider right now to be invasion of privacy and the disclosure of information that arises therefrom. From the standpoint of object abuse, where the abuse itself is the computer, conduct that may be criminal could be the unauthorized use of a computer system, the taking of a computer program, the taking of computer data, and in the interference with or damage to a computer or to its software.

• 1030

Of all those different activities, I would like to mention which ones I consider to be criminal conduct. I think anything that is fraud-related is criminal conduct, but in my opinion the Criminal Code already covers that. As far as mischief-related offences are concerned, where the computer is used as an

TÉMOIGNAGES

*(Enregistrement électronique)**[Traduction]*

Le jeudi 9 juin 1983

The Chairman: Order, please!

The sub-committee resumes consideration of its order of reference respecting computer crime.

This morning we have Mr. Stephen Georgas, a lawyer from Toronto, and also Mr. E.A. Tollefson, from the Department of Justice. Mr. Georgas will now make his presentation.

Nous lui souhaitons la bienvenue à Ottawa et nous le remercions d'avoir bien voulu accepter de venir nous aider à terminer cette étude importante.

M. Stephen Georgas (avocat à Toronto): Merci, madame le président.

Pour analyser le Bill C-667, j'ai choisi de déterminer quel était le comportement, comportement relatif aux ordinateurs, qui me semblait de nature criminelle; partant de là, j'ai cherché à déterminer si le Code criminel sous sa forme actuelle prévoyait ce type de comportement et, dans le cas contraire, dans quelle mesure le Bill Beatty corrige les lacunes.

En guise d'introduction, très rapidement, j'estime que pour déterminer si un comportement est criminel ou non, il ne faut pas poser pour principe que le droit criminel comble les lacunes qui pourraient exister dans d'autres secteurs du droit, par exemple les lois sur la propriété intellectuelle, sur les secrets commerciaux ou notre droit civil. Autrement dit, nous devons étudier exclusivement l'aspect criminel du comportement en cause.

Cela posé, j'ai essayé de déterminer quel type de comportement pouvait être considéré comme criminel dans le secteur de l'informatique. J'ai séparé deux types de comportement fondamentaux. Les cas où un ordinateur est utilisé comme instrument d'infraction et les cas où un ordinateur fait l'objet d'une infraction.

Dans la première catégorie, je mettrais les infractions de type frauduleux, les actes de malveillance, toutes les activités que nous considérons à l'heure actuelle comme une atteinte à la vie privée; toutes les communications d'information qui peuvent être faites partant de là. Quant aux infractions où l'ordinateur est l'objet même de l'infraction, un comportement criminel peut être l'utilisation non autorisée d'un système d'ordinateur, le vol d'un programme d'ordinateur, de données informatisées, l'accès non autorisé ou les dommages causés à un ordinateur et à son logiciel.

Parmi toutes ces activités différentes, je vais maintenant parler de celles qui me semblent constituer un comportement criminel. À mon sens, tout ce qui est frauduleux est un comportement criminel, mais le Code criminel embrasse déjà ce secteur. Quant aux délits de malveillance, les cas où

[Texte]

instrument and not the object of abuse, I think that is criminal conduct; but in my opinion that is also covered. I do not consider the invasion of privacy as it is defined in the Criminal Code to be criminal conduct, where you have a private communication and the computer is being used as an instrument to eavesdrop, so to speak. I think that is already covered anyhow.

But the disclosure of information where you have computerized data banks and there is some confidentiality associated with the data I would consider to be criminal conduct, and it does not appear to be covered by the Criminal Code as it now stands.

As for conduct where the object of the abuse is the computer itself, I would consider unauthorized use to be criminal conduct. The Criminal Code does not cover that right now. Similarly, the taking of computer programs I would consider as criminal but only to the extent that there is a proprietary nature associated with the computer program. What I am thinking of here is that if the computer program has fallen into the public domain or has become so widespread that it is readily available to all there may not be anything proprietary in it, and the same relates to data too.

As for interference and damage to a computer system or its software, I consider that to be criminal conduct, and the code right now does not cover that type of activity, at least from the software standpoint.

So, given those activities which I consider to be criminal, I would like to now discuss how Mr. Beatty's bill would cover them, just very briefly. It is not necessary to go into the fraud-related, mischief-related or invasion of privacy issues where the computer is used as an instrument of abuse simply because the code already covers it.

As far as disclosure of information is concerned, Mr. Beatty's bill does address that issue in a peripheral manner because it could be said that everyone who commits theft—and this is under his Clause 3, which would add a Section 283.1 to the Criminal Code: "283.1 Everyone commits theft . . ." etc., who " . . . diverts to his use . . . any computerized data."

So that possibly could cover the disclosure of confidential information, which I would be in favour of.

As for the computer used as an object of abuse, I do not think Mr. Beatty's bill covers the unauthorized use aspect and at most it is only done peripherally in proposed Section 283.1. But he does cover it in the taking of computer programs, the taking of computer data and the mischief provision. By amending Section 387, the interference with computer software is covered.

Looking at Bill C-667 in a bit more detail now, I would like to look at specific points.

[Traduction]

l'ordinateur sert d'instrument et non pas d'objet, cela me semble constituer un comportement criminel, mais c'est également prévu. Pour moi, les atteintes à la vie privée telles que définies dans le Code criminel ne constituent pas un comportement criminel lorsque des communications privées et les ordinateurs sont utilisés comme instruments d'écoute, pour ainsi dire. Et de toute façon, cela est déjà prévu.

Par contre, la communication d'informations par violation de banques de données informatisées considérées comme confidentielles est, à mon avis, un comportement criminel et, apparemment, le Code criminel actuel ne s'en occupe pas.

Quant au comportement où l'objet de l'infraction est l'ordinateur proprement dit, j'estime que, l'utilisation non autorisée constitue un comportement criminel. Le Code criminel ne vise pas ce domaine à l'heure actuelle. De la même façon, le vol de programme informatique peut être considéré comme criminel, mais uniquement dans la mesure où le programme informatique est la propriété de quelqu'un. Par exemple, il y a des programmes d'ordinateur qui sont tombés dans le domaine public ou qui sont tellement répandus que n'importe qui peut se les procurer, ce qui, à toutes fins pratiques, leur enlève le caractère de propriété privée; cela s'applique également aux données.

Quant à l'ingérence et aux dommages causés à un système d'ordinateur ou à son logiciel, cela me semble criminel et à l'heure actuelle, le Code ne prévoit pas ce type d'activité, du moins pas dans le cas du logiciel.

Voilà donc quelles sont les activités qui me semblent criminelles et je vais maintenant chercher à déterminer dans quelle mesure le bill de M. Beatty couvre ces secteurs. Inutile de s'attarder sur les comportements frauduleux, la malveillance ou les atteintes à la vie privée en cas d'utilisation de l'ordinateur comme instrument d'infraction, tout simplement parce que le Code s'occupe déjà de ces comportements.

Quant à la communication d'informations, le bill de M. Beatty traite de cette question d'une façon marginale puisque quiconque commet un vol, et c'est dans son article 3 qui compléterait l'article 283.1 du Code criminel: «283.1 Commet un vol, quiconque . . . » etc, « . . . détourne à son propre usage . . . toute donnée d'ordinateur. »

Par conséquent, ce serait une façon de protéger les informations confidentielles et cela me semble justifié.

Quant à l'ordinateur en tant qu'objet d'infraction, j'estime que le bill de M. Beatty ne prévoit pas l'utilisation non autorisée et, dans le meilleur des cas, il s'en occupe d'une façon marginale au projet d'article 283.1. Cela dit, il aborde le sujet à propos des programmes d'ordinateur, du vol de données informatiques et dans la disposition relative à la malveillance. En modifiant l'article 387, on règle le problème de l'ingérence dans le logiciel.

Maintenant, je vais me pencher d'un peu plus près sur le Bill C-667 et relever certains détails précis.

[Text]

• 1035

I have already covered the disclosure of information aspect. On the point of unauthorized use, this type of problem came up in the McLaughlin case in Alberta, and that case went to the Supreme Court of Canada. It appears to me that Section 283.1 does not cover it sufficiently. What I would suggest is something to the effect of repealing Section 287 of the Criminal Code and enacting it as follows: that it is an offence for anyone who uses any telecommunication or computer facility, or a combination thereof, or obtains any telecommunication or computer service, or combination thereof. The reason I put in the words "or combination thereof" is that in the McLaughlin case the Supreme Court of Canada focused on the functionality of the device, as to whether it was primarily used for computation or primarily used for telecommunications.

My concern is that in the future, in fact even now to a large extent, in some systems where there may be an abuse it may be difficult to say that the device was primarily used for telecommunications or primarily used for computation. I am thinking of message-switching systems which, for example, Bell Canada may be using, and yet in doing message switching you are also doing computation. If it was not legislated, as I am suggesting, that activity may fall between the cracks of Section 287.

As the bill and the Criminal Code stand right now, we would still have a valuation problem. In particular within Section 283.1 we would have to concern ourselves with the value of the computer program, and we are into the problem of are you going to value it according to the value of the medium, or value according to the intellectual property nature of it. The Code is silent on it and so is Bill C-667.

On the definitional matters, I have taken a look at the definition of "computer" and to a great extent I agree. My main concern is the exclusion of hand-held calculators. My reason being that there is an attempt here to define what I would consider one moving target in terms of another moving target. Computer technology is moving so quickly that whether the computer today may or may not be a computer 10 years from now . . . and certainly the courts can look to the facts at that time, and I appreciate that all statutes are living statutes, but we are defining a lower bound on computers, a lower bound being hand-held calculators. A calculator 10 years ago was not programable, and now they are programable; they are becoming close to what I would consider as computational, and they are hand-held. I do not know what is going to happen in the future, but I suspect that hand-held devices will become even more powerful than they are today. If that is the case, is such a device a calculator or a computer, and what is the difference? So I would just as soon have the exclusion of calculators removed from the definition.

In Clause 2.(b), the inclusion of computer software or programs; it may be that this is the right approach, not to define what computer software or programs are and allow the

[Translation]

J'ai déjà parlé de la communication d'informations. Quant à l'utilisation non autorisée, c'est un problème qui s'est posée à l'occasion de la cause McLaughlin en Alberta; cette affaire est allée jusqu'à la Cour suprême du Canada. J'ai l'impression que les dispositions de l'article 283.1 ne sont pas suffisantes. À mon sens, il faudrait abroger l'article 287 du Code criminel et le remplacer par ce qui suit: commet une infraction quiconque utilise des installations de télécommunication ou des installations informatiques ou d'une combinaison des deux, ou bien obtient des services de télécommunication ou d'ordinateur ou une combinaison des deux. Si j'ajoute l'expression «une combinaison des deux» c'est qu'à l'occasion de la cause McLaughlin, la Cour suprême du Canada s'est penchée plus particulièrement sur le caractère fonctionnel de l'appareil, s'est demandé s'il était utilisé avant tout à des fins de calcul ou avant tout à des fins de télécommunication.

Je crains qu'à l'avenir, et déjà aujourd'hui dans une large mesure, il ne soit difficile de déterminer dans quels cas, certains systèmes sont utilisés principalement à des fins de télécommunications ou principalement à des fins de calcul. Je pense aux systèmes de transmission de messages, ceux de Bell Canada par exemple, où il est possible de transmettre des messages tout en effectuant des calculs. Faute d'une législation dans ce domaine, je crains que ce type d'activité ne tombe précisément dans les lacunes de l'article 287.

Avec le bill et le Code criminel sous leur forme actuelle, il reste encore le problème de la valeur. En particulier, dans le cas de l'article 283.1, nous devons nous demander quelle est la valeur du programme d'ordinateur. Et cela nous amène à nous demander s'il faut déterminer la valeur selon la valeur du vecteur ou encore selon la valeur de la propriété intellectuelle. Le Code ne parle pas de cet aspect, pas plus que le Bill C-667.

Quant aux définitions, j'ai étudié la définition d'«ordinateur» et dans une large mesure, je suis d'accord. Ce qui me fait le plus peur, c'est l'exclusion des calculateurs ou autres petits appareils. En effet, j'ai l'impression qu'on a cherché à définir quelque chose d'insaisissable en se fondant sur quelque chose d'insaisissable. La technologie de l'informatique évolue si rapidement qu'il est difficile de dire aujourd'hui si ce qui est un ordinateur le sera encore dans dix ans. En tout cas, les tribunaux pourront toujours reconsidérer le moment venu. Je sais bien que les lois sont en évolution constante, mais comme nous cherchons à définir une limite inférieure pour les ordinateurs, cette limite inférieure, ce sont justement les calculateurs ou autres petits appareils. Il y a dix ans, les calculateurs n'étaient pas programmables; aujourd'hui, ils le sont. En fait, ils se rapprochent de plus en plus de ce que je considère comme un ordinateur et ils sont également portatifs. Je ne peux pas prévoir l'avenir, mais j'ai l'impression que les calculateurs portatifs vont continuer à se perfectionner. Et dans ce cas, comment faire la différence entre un calculateur et un ordinateur? Je préférerais donc qu'on supprime cette exclusion dans la définition.

Dans l'article 2.b), il est question de logiciel informatique ou de programmes; il est possible que cette démarche soit justifiée, qu'on ait eu raison de ne pas définir le logiciel

[Texte]

courts to decide that, because again the statute will live and that interpretation may change over the years. A possible suggestion is at least to provide some type of legislative guidelines on what software is, because it can mean different things to different people.

• 1040

For example, the committee may want to consider different types of software. One possible approach is that computer software relates to an algorithm before it is even reduced to a computer program form. And one algorithm that comes to mind, or I guess a law of nature, is the Pythagorean theorem, that in a right-angled triangle . . . the square of the hypotenuse is equal to the sum of the squares of its opposite sides. That is a mathematical truism, I guess.

That algorithm or equation can be reduced to source code, and I think most people are now acquainted with the notion of what source code is, that the source code is a series of instructions which a human being writes, and that source code can be in eye-readable form. It can also be encoded in machine-readable form. There are those two aspects to consider.

In addition, software could include optic code, which is a translation of the human beings series of instructions into machine-understandable instructions. Those machine understandable instructions can again be in machine-readable form or they can be in eye-readable form. They can be in eye-readable form in that many systems can provide printouts or, as the industry would classify it, a core dump or a memory dump of the optic code. That may be software.

The final possible inclusion is the computerized data itself. That has already been covered, I believe, in Mr. Beatty's definition, where he says: "... and retrievable computer data or information". That appears to be contemplated. One concern, by including information, is that until the information age, which many people consider to be our second industrial revolution—an information revolution—we were in a property regime where laws were enacted to protect property rights. Now, we are going into an information regime, and the question for the legislatures and the courts is: To what extent should information as a commodity be protected?

Clause 2.1(a) of the bill appears to contemplate the inclusion of information as property. It is qualified in that the information is produced and stored in machine-readable form by any means. In my opinion, that is a bold step, and a step that I do not think we should take right now. By redefining property in Section 2 of the Code to include information, we are affecting the entire Criminal Code. In my opinion, it might be a more prudent approach to legislate amendments, if Parliament sees fit to include information only in those sections relating to computer abuse. My reason for that is that I have not read the Criminal Code from cover to cover to see which sections of the code use the word "property". It may be

[Traduction]

informatique ou les programmes pour permettre aux tribunaux d'en décider. En effet, les lois sont appelées à évoluer et cette interprétation pourrait fort bien changer avec les années. Cela dit, on pourrait tout de même essayer de tracer des directives législatives sur la nature du logiciel, parce que cela peut avoir une signification différente selon les gens.

Par exemple, le Comité peut décider de faire la distinction entre différents types de logiciel. Une possibilité: pour être considéré comme un programme informatique, un logiciel d'informateur doit d'abord être lié à un algorithme. Un algorithme vient tout naturellement à l'esprit, peut-être faut-il il parler d'une loi de la nature, c'est le théorème de Pythagore selon lequel un triangle rectangle . . . le carré de l'hypoténuse est égal à la somme des carrés des deux autres côtés. C'est d'une vérité mathématique difficilement contestable.

Cet algorithme ou équation peut être réduit à un code de source et je pense que la plupart des gens savent aujourd'hui ce qu'est un code de source; c'est une série d'instructions rédigées par un être humain sous une forme lisible à l'oeil nu ou bien encore codées et repérables. Donc, deux possibilités.

De plus, le logiciel pourrait comprendre les codes optiques, une traduction de ces série d'instructions rédigées par des êtres humains en un langage qui peut être compris par la machine. Ces instructions intelligibles pour la machine peuvent être sous forme repérable ou encore sous forme lisible. En effet, beaucoup de systèmes fournissent des imprimés lisibles à l'oeil nu, ou encore ce qu'on appelle en jargon une banque centrale ou un mémoire du code optique. Tout cela peut être du logiciel.

Enfin, une dernière possibilité, les données informatiques proprement dites. Je crois que la définition de M. Beatty couvre déjà suffisamment ce secteur puisqu'il dit: "... ou programmes d'ordinateur, et l'information entrée sous une forme repérable". Cela semble donc être couvert. Cela dit, jusqu'au début de l'ère de l'information—et beaucoup de gens considèrent que c'est notre deuxième révolution industrielle, la révolution de l'information—nous vivions sous le régime de la propriété et les lois servaient à protéger la propriété privée. Aujourd'hui, nous entrons dans un régime de l'information et les législatures et les tribunaux vont devoir déterminer dans quelle mesure l'information, considérée comme un bien, doit être protégée.

A première vue, l'article 2.1a) du projet de loi considère que l'information est une forme de propriété. À cette réserve près que l'information est produite et emmagasinée sous forme repérable par n'importe quel moyen. À mon sens, c'est un peu aventureux, et nous ne devrions pas franchir ce pas aussi vite. En redéfinissant la propriété dans l'article 2 du Code pour y inclure l'information, nous modifions l'ensemble du Code criminel. À mon sens, il serait probablement plus prudent de commencer par des amendements puis, si le Parlement le juge indiqué, de ne parler d'information que dans les articles relatifs aux infractions en matière d'informatique. La raison pour laquelle je dis cela, c'est que je n'ai pas lu le Code

[Text]

that only the sections that we are considering do, but I think until someone does so, that step should be taken a little bit more cautiously.

• 1045

In Bill C-667 there are two pieces of terminology that we should consider, the words "data", and "information". We should try to understand what those two words mean. In my own mind, I consider information as being everywhere. It exists; it always existed and will always continue to exist. For example, the Pythagorean theorem, which I referred to before, existed long before Pythagoras reduced it to paper or stone. Newton's three laws existed long before Newton reduced those laws to paper. They are there. However, "data" is a bit different in my opinion, in that data relates to a compilation of information, and that compilation requires some effort by human beings, or machines.

An example is the telephone book. There are hundreds of thousands of names in the telephone book and there is nothing proprietary, in my opinion, in a name, but there is something proprietary, in other words copyright in this case, in the telephone book. Someone made an effort to compile the book, using information available to everybody, and that is a reduction of information to data.

So I just want to make that distinction, and it is my hope that that distinction will enable the legislature to better understand both this bill and any amendments to the code.

With respect to Section 283.1 the offence relates to a taking or diversion of all or part of a computer program or copy thereof, or any computerized data, provided that the accused has certain elements in his mind; namely the elements of fraud that he did so without colour of right.

What I submit that the committee should be aware of is that if there is nothing proprietary in those computer programs, and this may happen in the future, then the accused may still be guilty where he has the two elements in his mind of fraud and that he did so without colour of right. That is a concern. I do not think that should happen. There must be something proprietary in the computer program, or in the computerized data. I have already mentioned that proposed Section 283.1 is unclear as to whether it applies to an unauthorized use of a computer system and have suggested possible amendment to proposed Section 287 to cover that.

• 1050

As far as proposed Section 387.1(b), Bill C-667 is concerned, I find no problem with the section.

On Section 385, as it is defined, I make the same comment as I did relative to Clause 2 as to the inclusion of information

[Translation]

criminel de la première à la dernière page pour voir quels articles utilisaient le terme «bien». Il se pourrait que seuls les articles qui sont envisagés ici le fassent, mais avant de prendre une décision, je pense que l'on devrait réfléchir un peu plus prudemment à cette question.

Dans le projet de loi C-667, il y a deux termes que l'on doit regarder de près, ce sont les termes «data», (données), et «information» (information). Je pense qu'il faut chercher à comprendre la signification de ces termes. D'après moi, l'information se trouve partout. Elle existe, tout simplement; elle a toujours été là, et elle continuera à l'être. Prenons l'exemple du théorème de Pythagore, dont je parlais tout à l'heure; il existait bien avant que Pythagore en fasse quelque chose sur le papier, ou sur la pierre. Les trois lois de Newton existaient également bien avant Newton. Ces éléments sont là. Toutefois, «data» (données) représente quelque chose d'un peu différent, à mon avis, dans la mesure où il s'agit d'informations rassemblées, ce qui demande un travail, fourni par l'homme ou la machine.

Prenons l'exemple de l'annuaire téléphonique. Il y a des centaines de milliers de noms dans ce volume, or le nom n'est pas quelque chose qui implique un rapport de propriété—à mon avis—alors qu'il y a tout de même dans cet annuaire une question de droit d'auteur qui intervient, et qui implique donc un rapport de propriété. Pour produire ce livre, il a fallu un travail, il a fallu faire les listes, utiliser de l'information disponible, et réduire cette information en données.

Voilà donc une distinction que je voulais faire, et j'espère que cela permettra aux législateurs de mieux comprendre la portée de ce projet de loi et de tout amendement au Code criminel.

Le paragraphe 283.1 définit une infraction, consistant à prendre ou détourner totalité ou partie d'un logiciel, ou copie de logiciel, ou toute information, lorsque l'accusé le fait frauduleusement et sans apparence de droit, comme le dit l'article.

Or il convient d'attirer l'attention du Comité sur le fait que les logiciels ne sont toujours pas définis comme des biens, et que s'il en restait ainsi à l'avenir, l'accusé serait tout de même considéré comme coupable, s'il s'avérait qu'il avait agi frauduleusement et sans apparence de droit. Voilà donc un point à considérer. Je ne pense pas qu'il devrait en être ainsi. Il faut donc que l'on définisse le logiciel comme un bien, de même que l'information. J'ai déjà expliqué que le paragraphe 283.1 ne disait pas de façon claire s'il concernait l'utilisation non autorisée d'un système informatisé, et j'ai proposé à cet effet un amendement à l'article 287 qui permettrait d'y remédier.

Je n'ai aucune difficulté à accepter l'alinéa 387.1b) du projet de loi, tel qu'il est rédigé.

Je ferai à peu près les mêmes remarques à propos de l'article 385 que celles que j'ai faites à propos de l'article 2, en ce qui

[Texte]

as property but, here, it may be all right; here we are including information as property only for the purposes of the mischief provisions of the act or the Code and that may be the prudent way to go.

So my overall comments as far as the bill is concerned from the Criminal Code standpoint is that I am in favour of the general approach of legislating specific provisions, as far as computer abuse is concerned, with the exception of expanding the property notion in general to include information.

My next comments relate to the evidentiary matters covered in Clause 6 of the bill which proposes to enact the proposed Section 24.1 of the Canada Evidence Act. And in analysing Section 24.1 as it is proposed, I would like to make some comments about the draft Uniform Evidence Act as it was in 1981, and Bill S-33. I can use those comments to put proposed Section 24.1 into context. In the draft Uniform Evidence Act under its old Section 171.1(c) one of the requirements for the admissibility of computerized business records was that the program processing the information does so reliably and, I believe, accurately. I am just going to get a copy of that section and read it. Proposed Section 171.1(c) says:

A business record made by a computer is admissible in evidence in the same manner as any other business record, if the proponent proves that the computer program used in producing the record reliably and accurately processes the data or information in the data or information bank.

And when I looked at the section my concern was to which computer program does the section relate. Does it relate to the computer program or programs that manipulate the data within the machine? Or does it relate to the computer program which retrieves the data as it is stored in the machine, prints it out in a human readable form that is tendered into evidence? That was unclear at the time.

Bill S-33 appears to overcome that question in my mind anyhow, by defining "original" in relation to "stored or processed data" as any printout or intelligible output that reflects accurately the data or information, or is the product of a system that does so. So in principle I am in favour of that approach.

• 1055

On the issue of admissibility of computerized evidence, and I point out the word "admissibility", the legislature should be concerned with the accuracy of the computer program that creates the print-out. As to the accuracy of the computer program or programs that have manipulated the data within the system, in my opinion that goes to credibility, to the weight or probit of value that is to be associated with the data. Mr. Beatty's bill tends to follow this latter approach, because it says:

... "original", when used in relation to data stored in a form readily accessible to a computer, includes a printout or

[Traduction]

concerne l'inclusion de l'information dans la définition de «bien», bien que cela semble possible ici, de cette façon; l'information est considérée comme bien aux fins des dispositions concernant le méfait dans la loi, ou dans le Code, et il est sans doute prudent de procéder ainsi.

De façon générale, donc, je suis d'accord avec l'approche proposée par ce projet de loi quant au Code criminel, ainsi qu'avec les dispositions concernant les infractions possibles commises lors de l'utilisation d'un ordinateur, excepté cette définition du terme «bien» qui inclurait l'information.

Je vais maintenant discuter de la preuve, dont il est question à l'article 6, qui propose que l'on ajoute le paragraphe 1 à l'article 24 de la Loi sur la preuve au Canada. J'aimerais, à ce sujet, revenir à la Loi uniforme sur la preuve, ce document de 1981 que reprend le projet de loi S-33. Cela nous permettra de remettre le paragraphe 24.1 en perspective. Une première version de l'alinéa 171.1(c) du document sur la loi uniforme sur la preuve exige, pour que les documents commerciaux ou professionnels informatisés soient recevables, que le programme dont on s'est servi pour les produire se soit avéré fidèle. Je vais me référer à cet article et vous le lire. Il s'agit de l'alinéa 171.1(c):

Une pièce d'affaires qui provient d'ordinateur est admissible en preuve, aux mêmes conditions que toute pièce d'affaires, si celui qui entend s'en servir établit que la programmation de l'ordinateur utilisé pour produire cette pièce effectuée correctement et précisément le traitement des données contenues dans la banque.

À la lecture de cet alinéa, je me suis posé la question de savoir de quel programme d'ordinateur il s'agissait. S'agit-il du programme de l'ordinateur, ou des programmes qui permettent d'effectuer des opérations sur les données, à l'intérieur des systèmes informatisés? Ou s'agit-il, au contraire, du programme de l'ordinateur qui permet de retrouver les données emmagasinées, et d'en faire des états mécanographiés, que chacun peut lire, et que l'on fournira pour preuve? Cela me semblait très peu clair.

Le projet de loi S-33 semble résoudre cette question, à mon avis du moins, en définissant «l'original», en fonction des «données emmagasinées ou traitées» comme étant n'importe quel état mécanographié, ou document imprimé compréhensible, reproduisant fidèlement les données ou l'information, ou tout autre produit de la machine qui remplit ces conditions. En principe, je suis donc partisan de cette conception.

En ce qui concerne cette question de la recevabilité des preuves produites par ordinateur, et je souligne le terme «recevabilité», la loi devrait surtout s'assurer que le programme de l'ordinateur permet de produire des états mécanographiés fidèles. Cette question de fidélité du programme ou des programmes qui ont traité les données à l'intérieur du système informatisé, engage la question de la crédibilité, du poids ou de la valeur probante de ces éléments de preuve. Le projet de loi de M. Beatty semble s'orienter dans ce sens, puisqu'il précise:

... «l'original» des données entrées sous une forme facilement repérable par ordinateur s'entend notamment d'un état

[Text]

other machine-readable output shown to reflect the data accurately.

So if that were the case, and that approach becomes law, the person tendering the evidence would have to show, and this could possibly be done by affidavit evidence, that the program that was used to create that print-out accurately reflects the data in the system, the evidence gets in. Once it is in, it is now up to the judge and the two parties to establish a weight to the information contained on the printer, and you can consider a whole series of factors for that.

The common law notions of business records may be contemporaneity; how many conversions of the data occurred since the time that, let us say, the master files were first encoded on the system and from that time until the time that the program created the print-out that is tendered into evidence, how many conversions occurred in that period of time; how many times the institution whose computer stored the data had to run fixes, if you want to call them that, special programs to make sure that everything balances. All those considerations, in my opinion, should go to the probit of value and not to the issue of admissibility. As I have said, proposed Section 24.1 seems to contemplate that.

One concern, and this may be a slip, is that it says:

In every case where an original is required for evidence . . . , "original", . . . includes a printout or other machine-readable output . . .

I would suggest that you do not want machine-readable output, you would want human-readable output, if that is what is going to be tendered into evidence. A print-out is human-readable and presumably other . . . It is something else, it is going to be other human-readable output rather than machine-readable output; and that may have just been a slip by the draftsman.

The other comment I would like to make about proposed Section 24.1 is that it relates to original and it gets away from the notion of computerized business records. I am in favour of that approach, because in going back to the draft Uniform Evidence Act, one of the problems I had in reading it was trying to understand what a computerized business record is. It . . . to have all the same features as a business record in our traditional common law stance. I would have difficulty in determining what it is in a computer, and I think it on that point it is important to understand how data is stored in a computer, because data is not necessarily stored in continuous blocks.

[Translation]

mécanographié ou autre document produit de données informatisées qui reflète fidèlement lesdites données.

Si donc cette disposition devait entrer en vigueur, la personne fournissant des éléments de preuve devrait également établir, et cela pourrait donner lieu à une déclaration faite sous serment, que le programme utilisé produit des états mécanographiés reflétant fidèlement les données emmagasinées, et alors les déclarations sont retenues comme élément de preuve. Cela fait, il appartient ensuite au juge et aux parties en présence d'évaluer le poids qu'il convient de donner à ces renseignements fournis par l'état mécanographié, et toutes sortes de facteurs peuvent être pris en compte pour ce faire.

Aux termes de la *Common law*, on peut ensuite faire entrer en ligne de compte des questions de simultanéité de la production des documents, ou de succession dans le temps, c'est-à-dire combien de conversions des données ont pu avoir lieu entre le moment où les originaux ont été mis sur ordinateur et celui où le programme a permis de produire des états mécanographiés dont on se sert comme éléments de preuve; ou bien, combien de fois la firme responsable de l'ordinateur a dû faire des réparations, si vous voulez, c'est-à-dire recourir à des programmes spéciaux supplémentaires qui permettent de vérifier que tout est en ordre. Toutes ces considérations, à mon avis, relèvent de l'appréciation de la valeur des éléments de preuve, et non pas de la recevabilité à proprement parler. Comme je le disais, le paragraphe proposé 24.1 semble répondre à cette question.

J'ai tout de même une réserve, et c'est peut-être une erreur qui a échappé au rédacteur, lorsqu'il précise:

Dans tous les cas où la pièce originale est requise pour qu'un document soit admissible, «l'original», . . . s'entend notamment d'un état mécanographié ou autre document produit de données informatisées . . .

Je pense qu'en fait ce que vous voulez, ce ne sont pas des documents qui puissent être lus par une machine, mais plutôt que toute personne puisse lire, si on doit s'en servir comme éléments de preuve. Je pense qu'un état mécanographié peut être lu par n'importe qui, et que . . . Je pense donc que l'on parlera d'état mécanographié compréhensible pour toute personne, et pas seulement utilisable par la machine; cela est peut-être tout simplement une faute d'inattention du rédacteur.

Je voudrais ajouter que ce paragraphe proposé 24.1 nous parle de l'original, sans parler de pièces d'affaires informatisées. Je suis partisan de cette nouvelle approche, étant donné que j'avais des difficultés à comprendre exactement ce qu'une pièce d'affaires informatisée pouvait être, dans la Loi uniforme sur la preuve. S'agissait-il d'une pièce d'affaires comme notre *Common law* traditionnel la définit? J'avais du mal à comprendre quel pouvait en être l'équivalent en termes d'informatique, et il est important, à ce propos, de pouvoir comprendre comment les données sont mises sur ordinateur, étant donné qu'elles ne se trouvent pas nécessairement sous forme de blocs continus.

[Texte]

• 1100

Nowadays, systems are implemented in a data base concept, so you would have separate logical files of information which inter-relate with other separate logical files to create a business record, in a traditional sense. For example, an invoice. If I use the analogy of a commercial invoice, the name and address at the top of the invoice may come from a name and address file, whereas the items in the body of the invoice may come from a totally different file; it could be an open item file, for example. So it could be said that this paper document, the invoice, is manufactured and is not a business record within our traditional notions. Proposed Section 24.1 gets away from that because it is just looking at originals, and with that I am in favour.

Those are the comments I have on Bill C-667. Thank you.

The Chairman: Thank you. Do you think we can proceed with questions while the bell is ringing?

Mr. Beatty: Thank you, Madam Chairwoman. I have no questions.

The Chairman: Mr. Robinson?

Mr. Robinson (Etobicoke—Lakeshore): Yes. Mr. Georgas, you say you have not looked at all the sections of the Criminal Code that might be changed.

Mr. Georgas: That is correct.

Mr. Robinson (Etobicoke—Lakeshore): You have just looked at a few, and you have enumerated the ones that you have looked at. There may be others. We had before us yesterday the Canadian Bar Association and they have been looking at them. They came up with a draft section for the Criminal Code which they would call 394(a)(1), and if you would like to take a look at that when you get the opportunity, you might indicate to us whether you agree or disagree with the extent to which they have gone in trying to define such things as computer, computer program, computer software, computer system, and the rest of that draft section. Even though it would not necessarily be all-inclusive of their recommendations, it was what they considered a draft form that might be of assistance in amending the Criminal Code. I would be interested in having your comment. I realize you may not have seen this before, but I would appreciate having your comment with regard to it.

• 1105

Mr. Georgas: I am going to cheat a little bit and look at some other definitions that I have, just by means of a comparison.

With respect to the definition of computer, one comment is that you should look at just the last phrase: The results of the operation. From a technical drafting standpoint, there is no antecedent for "operation". In other words, it should relate to "an" operation.

Mr. Robinson (Etobicoke—Lakeshore): It should be the word "an" instead of the word "the".

[Traduction]

Aujourd'hui, les systèmes informatisés font appel à la notion de base de données, faisant jouer différents ensembles logiques d'informations, interconnectés et permettant de produire la pièce d'affaires ou le document commercial, comme on l'entend dans un sens traditionnel. Prenons l'exemple d'une facture. Le nom et l'adresse, en haut, viendront d'un dossier contenant des noms et des adresses, alors que les chiffres et intitulés de la facture seront produits par un autre dossier d'informations; on pourrait également en avoir sans spécification. On peut donc dire que ce document en papier, la facture, est un produit manufacturé, plutôt qu'un document commercial dans le sens traditionnel. Le paragraphe 24.1 proposé laisse donc cela de côté, puisqu'il s'intéresse simplement aux originaux, et je suis partisan de cette solution.

Voilà donc ce que je voulais dire sur le Bill C-667. Merci.

Le président: Merci. Pensez-vous que nous puissions poser des questions pendant que la cloche sonne?

M. Beatty: Merci, madame le président. Je n'ai pas de question.

Le président: Monsieur Robinson?

M. Robinson (Etobicoke—Lakeshore): Oui. Monsieur Georgas, vous dites que vous n'avez pas examiné tous les articles du Code criminel qu'il faudrait peut-être changer.

M. Georgas: En effet.

M. Robinson (Etobicoke—Lakeshore): Vous en avez simplement regardé certains, que vous nous avez cités. Il pourrait y en avoir d'autres. L'Association du Barreau canadien a comparu hier, et ils nous en ont parlé. Ils ont entre autres proposé un nouvel article au Code criminel, ce serait la disposition 394a(1), et si vous voulez vous y reporter quand vous en aurez la possibilité, vous pourrez nous dire ce que vous en pensez, et notamment la définition qu'ils proposent de termes tels qu'ordinateur, programme d'ordinateur, logiciel, système informatisé, et cetera. Cette proposition d'article n'épuise pas les recommandations qui nous ont été faites, le Barreau pensait simplement que cela pourrait nous aider si nous voulions remanier le Code criminel. J'aimerais savoir ce que vous en pensez. Peut-être pourrez-vous vous y reporter.

M. Georgas: Je vais tricher un peu et consulter d'autres définitions pour faire une comparaison.

Pour ce qui est de la définition d'ordinateur, il suffit de tenir compte de la fin de la phrase: les résultats de l'opération. Du point de vue de l'analyse grammaticale, il n'y a pas d'antécédent pour «opération». Autrement dit, ce dont il est question, c'est d'une opération.

M. Robinson (Etobicoke—Lakeshore): Autrement dit, il faudrait remplacer le mot «l» par «une».

[Text]

Mr. Georgas: Certainly the indefinite article.

Mr. Robinson (Etobicoke—Lakeshore): Yes. I would agree with that.

Mr. Georgas: What is the requirement for the word "automatically" in "a computer capable of automatically accepted data"?

Mr. Robinson (Etobicoke—Lakeshore): I think, Mr. Georgas, you have answered the query that I wanted to make, and that is that although the Canadian Bar Association has come up with some definition and a draft section, it is probably something that needs to be looked at and looked at carefully by people who are in the business of drafting legislation. It may contain some good ideas but it is subject, maybe, to drafting errors and maybe some inconsistencies. So I will not ask you further about that, but it is something you may wish to take away with you and maybe, if you have some suggestions with regard to this, you might send them to us. We would be glad to receive any assistance we can.

Mr. Georgas: Certainly.

Mr. Robinson (Etobicoke—Lakeshore): Our time is very short, so I want to go on to two or three other things here.

Mr. Georgas: Okay.

Mr. Robinson (Etobicoke—Lakeshore): One in particular is; You have a tendency, I think, in your statement, to show a difference between property rights and information rights.

Mr. Georgas: Yes.

Mr. Robinson (Etobicoke—Lakeshore): You have indicated, in effect, that one came before the other. We went through the property revolution and now the information revolution and there seems to be a tendency maybe to try to put the two together. In your view it appears that they do not necessarily mix, but rather there should properly be separate sections covering property rights and separate sections covering information rights.

Mr. Georgas: I think that is a fair statement. In fact, if you look at the invasion of privacy provisions of the code as it now stands, those sections, I believe, contemplate information. Disclosure of information. Yes. In fact, Section 178.2 . . .

Mr. Robinson (Etobicoke—Lakeshore): So, really, what you are saying is that you do not feel it is satisfactory just to try to include in the definition of property, information?

Mr. Georgas: That is correct.

Mr. Robinson (Etobicoke—Lakeshore): All right. Now, when you talk about information, I think you have used a rather large definition, because I think, first of all, you wanted to distinguish between information and data and I would assume that when you speak of information, you are including data. Would that not be a fair statement?

The Chairman: Can I be of help?

Mr. Georgas: Yes.

The Chairman: Well, maybe I could suggest to Ken, since we have been struggling with words, that my understanding of

[Translation]

M. Georgas: Absolument, l'article indéfini.

M. Robinson (Etobicoke—Lakeshore): Oui. Je suis d'accord.

M. Georgas: Quelle est l'utilité du terme «automatiquement» dans la phrase «un ordinateur capable d'accepter automatiquement des données»?

M. Robinson (Etobicoke—Lakeshore): Monsieur Georgas, je crois que vous avez déjà répondu à la question que j'allais poser, bien que l'Association du Barreau canadien ait préparé des définitions et un projet d'article, c'est quelque chose qui va devoir être encore approfondi par les rédacteurs de lois. Il y a probablement de bonnes idées là-dedans, mais les erreurs de rédaction sont possibles et il y a peut-être encore certaines contradictions. Je vais donc en rester là, mais vous pourriez peut-être continuer à y réfléchir et si vous avez des suggestions à ce sujet, vous pourriez nous les envoyer. Nous vous serons toujours reconnaissants de votre aide.

M. Georgas: Je n'y manquerai pas.

M. Robinson (Etobicoke—Lakeshore): Nous sommes très pressés par le temps et je veux aborder deux ou trois autres questions.

M. Georgas: D'accord.

M. Robinson (Etobicoke—Lakeshore): En vous écoutant, j'ai eu l'impression que vous faisiez volontiers une différence entre le droit de propriété et le droit sur l'information.

M. Georgas: Oui.

M. Robinson (Etobicoke—Lakeshore): En fait, pour vous, l'un l'emporte sur l'autre. Nous sommes passés par une révolution de la propriété et aujourd'hui nous en sommes à la révolution de l'information; malgré tout, on a souvent tendance à les assimiler. Vous estimez, de votre côté, que les deux ne vont pas forcément ensemble et que normalement des articles différents devraient être consacrés au droit de propriété et au droit sur l'information.

M. Georgas: C'est bien ça. En fait, si vous lisez les dispositions relatives aux atteintes à la vie privée dans le Code actuel, vous verrez que l'information est mentionnée. La communication d'informations. En fait, l'article 178.2 . . .

M. Robinson (Etobicoke—Lakeshore): Par conséquent, pour vous il n'est pas suffisant d'essayer d'ajouter l'information à la définition de la propriété?

M. Georgas: Absolument.

M. Robinson (Etobicoke—Lakeshore): Très bien. Maintenant, à propos de l'information, vous donnez une définition qui semble assez large puisque vous commencez, je pense, par faire une distinction entre l'information et les données. J'imagine que lorsque vous parlez d'information, vous parlez également des données. C'est bien cela, n'est-ce pas?

Le président: Vous me permettez d'intervenir?

M. Georgas: Oui.

Le président: J'ai une suggestion pour Ken; puisque nous semblons avoir des difficultés avec les mots, j'ai cru compren-

[Texte]

your comments was that information being all over the place, the data appears when it is an organized fashion.

Mr. Georgas: That is correct.

The Chairman: You necessarily have information in data, but information is not necessarily data.

Mr. Georgas: That is correct.

The Chairman: Okay. So, I think, for the purpose, I think data is something that is usually organized and is in the computer. Once it is organized, programmed and inserted in a fashion that you can retrieve it, then it becomes data. That is my understanding of what data is.

Mr. Georgas: Yes. That is also my understanding.

• 1110

The Chairman: I have a lot of information in the printed press, but it is not necessarily data I can find there.

Mr. Georgas: Sure.

Mr. Robinson (Etobicoke—Lakeshore): Would you say that you create data but not information?

Mr. Georgas: Yes, I would say that. Maybe by example, so we can put it into context: We can all, or we should all, know what the 10 provinces of Canada are and their corresponding capitals. But if I sit down and, starting with the Province of British Columbia and going east to the Province of Newfoundland, write them down on a piece of paper with their corresponding capitals, I would suggest to you that I have taken information and reduced it to data. Some effort, some compilation has gone into it.

Mr. Robinson (Etobicoke—Lakeshore): You made the statement that in your view the invasion of privacy was not, in itself, criminal conduct.

Mr. Georgas: I had better be careful when I say that, because it is criminal conduct in that it is already legislated. With the invasion of privacy, we are talking about private communications here. What I am getting at is whether you use a computer to invade the privacy of two persons who have a private communication or use some other electromagnetic means does not matter, it is already covered.

Mr. Robinson (Etobicoke—Lakeshore): But you would appreciate, I am sure, that all federal statutes are really criminal in nature...

Mr. Georgas: Yes.

Mr. Robinson (Etobicoke—Lakeshore): —there is a record and there is a penalty and so on. Would you prefer that the matter of so-called computer crime be dealt with in a different way, say through provincial legislation? In other words, is there any approach that you feel should be taken, other than through amendments to the Criminal Code? What about other federal statutes as well, like the Copyright Act, the Patent Act and so on?

[Traduction]

dre que pour vous, l'information était partout mais qu'elle ne devient données que lorsqu'elle est organisée.

M. Georgas: Exactement.

Le président: Les données sont forcément de l'information mais l'information n'est pas forcément une donnée.

M. Georgas: Présisément.

Le président: D'accord. Ainsi, à toutes fins utiles, les données sont d'ordinaire organisées et rangées dans un ordinateur. Une fois organisées, programmées et entrées sous une forme repérable, elles deviennent données. Voilà comment je comprends les données.

M. Georgas: Oui, moi aussi.

Le président: J'ai beaucoup de renseignements de la presse écrite, mais je ne peux pas nécessairement les trouver là.

M. Georgas: Certainement.

M. Robinson (Etobicoke—Lakeshore): Diriez-vous que vous créez des données mais pas de l'information.

M. Georgas: Oui. Je vais vous donner un exemple pour que nous mettions la chose en perspective: Nous connaissons tous, ou tout au moins nous le devrions, les dix provinces du Canada ainsi que chacune des capitales provinciales. Si j'écris sur une feuille de papier en commençant par la Colombie-Britannique jusqu'à Terre-Neuve le nom des provinces avec leur capitale correspondante, j'ai transformé de l'information en données. Cette opération a nécessité une certaine compilation de données.

M. Robinson (Etobicoke—Lakeshore): Vous avez dit que selon vous la violation de la vie privée n'était pas en soi une infraction criminelle.

M. Georgas: Je devrais être prudent en disant cela, car il s'agit d'une infraction criminelle en ce sens qu'elle est déjà sanctionnée par la loi. Quand nous parlons de violation de la vie privée, nous parlons de communication privée. Ce que je veux dire c'est que peu importe si vous vous servez d'un ordinateur pour violer le caractère privé d'une communication entre deux personnes ou que vous utilisiez certains autres moyens électromagnétiques, peu importe, c'est déjà prévu.

M. Robinson (Etobicoke—Lakeshore): Mais je suis sûr que vous vous rendez compte que toutes les lois fédérales sont à vrai dire des lois qui sanctionnent...

M. Georgas: Oui.

M. Robinson (Etobicoke—Lakeshore): Les infractions sont enregistrées et punies etc. Préféreriez-vous que ce que l'on appelle les délits informatiques soient traités d'une façon différente, disons qu'ils seraient sanctionnés par les lois provinciales? En d'autres termes, y aurait-il selon vous une autre façon de procéder plutôt que de modifier le Code criminel? Pourrait-on faire intervenir d'autres lois fédérales également comme la Loi sur le droit d'auteur ou la Loi sur les brevets etc.?

[Text]

Mr. Georgas: I understand that the Copyright Act, in particular, has some penalties in it for copyright infringement.

The question that Parliament has to consider... and I attempted to make the point at the beginning of my presentation—is, is certain conduct criminal in nature? If it is, it falls within the realm of the criminal law; if it is not, some other type of legal means of enforcing these other rights that are affected should be used. You should not just say that with computer software it is difficult to enforce my remedies through copyright or trade secrecy or patent; we all know that there are weaknesses in those pieces of legislation, therefore, let us use the criminal law. I would not take that approach. I would ask: Is a certain type of activity something that is criminal? In my view, the items of conduct, the different types of conduct that I mentioned, are types of conduct that one should consider as criminal. Whether another federal statute contemplates it from a different approach is something totally different, or a provincial government as well, from a proprietary standpoint.

Mr. Robinson (Etobicoke—Lakeshore): You mentioned, when you were discussing Section 283.(1), that in your view if there were no proprietary aspect in a computer program there should not be any offence. In other words, are you saying that you eliminate the whole question of *mens rea* altogether?

Mr. Georgas: No, not at all. What I am saying in that is that I am looking to make sure that there is something proprietary in that thing taken. I will use an example of a little computer program that is published in a book for everyone to use on a calculator, let us say, or one of the personal computers, a computer program that is readily available and is extremely simple.

• 1115

I encode that program in my system, and you come along and take it. I suggest to you that I do not have any proprietary right in that computer program. It is available to all.

Mr. Robinson (Etobicoke—Lakeshore): But are we not really talking about the accessing to the information, not just the information itself? Is not the doing of the act itself the crime? Whether the material is of value or not...

Mr. Georgas: That is a different consideration.

Mr. Robinson (Etobicoke—Lakeshore): That is a different consideration; exactly.

Where do we draw the line in this? Are you suggesting that you can access all you like, as long as you do not take something of value?

Mr. Georgas: No, I am not suggesting that.

Has that program I have just referred to not fallen into the public domain, for example? If it has, why should it be a

[Translation]

M. Georgas: Je pense que la loi sur le droit d'auteur notamment prévoit certaines sanctions pour infraction aux droits d'auteur.

Le Parlement doit se poser la question de savoir, et j'ai essayé de le dire au début de ma déclaration... si certains actes sont criminels par nature? Dans l'affirmative, ces actes relèvent du droit criminel, dans le cas contraire, il faudrait recourir à d'autres mesures juridiques pour faire respecter les droits qui ont été enfreints. Vous ne devriez pas vous borner à dire que pour le logiciel informatique, il est difficile de faire respecter les mesures que je propose par le biais de la Loi sur le droit d'auteur, la Loi sur les secrets commerciaux ou la Loi sur les brevets; nous savons tous en effet que toutes ces lois comportent des lacunes, en conséquence, servons-nous du droit criminel. Je ne suivrais pas cette méthode. Je poserais la question suivante: Est-ce que certaines activités peuvent être considérées comme des activités criminelles? À mon sens, différents types d'actes dont j'ai parlé devraient être considérés comme des actes criminels. Maintenant, du point de vue de la propriété, si d'autres lois fédérales où un gouvernement provincial considèrent ces actes différemment, c'est une autre affaire.

M. Robinson (Etobicoke—Lakeshore): Lorsque vous discutiez du paragraphe 283.(1) vous avez dit que selon vous que si un programme informatique n'est pas une propriété, il ne devrait pas y avoir d'infraction. En d'autres termes, est-ce que vous éliminez toute la question de la «*mens rea*»?

M. Georgas: Non pas du tout. En disant cela, je dis que je veux m'assurer que ce qui a été dérobé est en fait une propriété. Je vais vous donner l'exemple du programme d'un petit ordinateur publié dans un livre pour que tous les intéressés puissent s'en servir avec une calculatrice, ou encore avec un ordinateur personnel, il s'agit d'un programme informatique que l'on trouve partout et qui est extrêmement simple.

J'encode ce programme dans mon système, et vous me le dérobez. Dans ce cas je dirais que je n'ai aucun droit de propriété sur ce programme informatique. Tout le monde peut s'en servir.

M. Robinson (Etobicoke—Lakeshore): Mais la question ne porte-t-elle pas plutôt sur l'accès à l'information plus que sur l'information en soi? L'infraction ne découle-t-elle pas du fait que le geste a été posé? Peu importe que le logiciel ait une certaine valeur ou non...

M. Georgas: C'est quelque chose de différent.

M. Robinson (Etobicoke—Lakeshore): C'est quelque chose de différent; exactement.

Où se situe la ligne de démarcation? Dois-je comprendre que vous dites que dans la mesure où l'on ne dérobe rien qui soit de valeur, on peut avoir accès à n'importe quoi?

M. Georgas: Non, je ne dis pas cela du tout.

Le programme dont je viens de parler, par exemple, n'est-il pas maintenant du domaine public? Si c'est le cas, pourquoi le fait de s'en servir devrait-il être considéré comme un acte

[Texte]

criminal act to take it—*mens rea* aside; that is a totally separate issue.

Mr. Robinson (Etobicoke—Lakeshore): Maybe I could ask you this. Insofar as any changes in the Canada Evidence Act are concerned—and you referred to the Canada Evidence Act . . . and the proposed Bill S-33, do you feel that in the case of computer crime or anything related to it the best evidence rule would still apply? If the best evidence rule applies, what would be considered as best evidence when you are talking about computers? Are you talking about the computer program itself, the software, or a copy of it?

Mr. Georgas: The best evidence rule, in my opinion, should still apply.

Mr. Robinson (Etobicoke—Lakeshore): When you were talking about admissibility, you mentioned the question of reliability. Do you equate reliability with credibility?

Mr. Georgas: No. There are two issues in considering computerized evidence. The first one is the issue of admissibility; just getting the evidence into court. On that point, in my opinion you should look at just the computer program that prints out the data stored in the machine.

Mr. Robinson (Etobicoke—Lakeshore): On the issue of admissibility?

Mr. Georgas: That is correct, yes.

The issue of credibility, in my opinion, is something totally different. On that issue of credibility, one would look at the computer programs that manipulated the data over the course of months, the conduct of the institution that ran the computer system, and possibly even the length of time the data was stored in the machine. But the issues are different, and there are two of them.

Mr. Robinson (Etobicoke—Lakeshore): Could I ask you this—and this is my final question . . . proposed Section 159 of this Bill S-33, concerning where probative force is not included, states:

Where enactment other than this act provides that a record is evidence of a fact without anything in the context to indicate the probative force of that evidence, the record is proof of the fact in the absence of evidence to the contrary in any proceeding to which this act applies.

How do you see this in terms of the matter we have before us, computer crime? Should anything be added or deleted, or is this satisfactory?

• 1120

Mr. Georgas: To paraphrase proposed Section 159 . . . correct me if I am wrong in reading it—it is saying that if there is another piece of legislation evidence will be believed without looking at its probative value in the absence of anything to the contrary. If that legislation is in place, then the Canada Evidence Act or Bill S-33 would give effect to that. Is that not the correct understanding?

[Traduction]

criminel . . . *mens rea* à part; c'est une question tout à fait différente.

M. Robinson (Etobicoke—Lakeshore): Je pourrais peut-être vous poser la question suivante: en ce qui a trait à tout changement à la Loi sur la preuve au Canada—vous en avez parlé—et au projet de loi S-33, pensez-vous que dans le cas de truandique et ses corrolaires, la règle de la meilleure preuve continuerait de s'appliquer? Si cette règle s'applique, selon vous quelles seraient les preuves les plus probantes en parlant de truandique? Est-ce que ce serait le programme en soi, le logiciel ou une copie?

M. Georgas: La règle de la meilleure preuve à mon avis devrait toujours s'appliquer.

M. Robinson (Etobicoke—Lakeshore): Quand vous parliez de preuves admissibles, vous avez abordé la question de la fiabilité. Pour vous fiabilité et crédibilité sont-elles une et même chose?

M. Georgas: Non. Il s'agit de deux choses différentes en ce qui concerne les truandiques. La première a trait à l'admissibilité, c'est-à-dire pouvoir présenter les faits en cour. À partir de là, à mon sens, vous devriez jeter un coup d'oeil au programme informatique qui permet d'imprimer les données emmagasinées dans l'ordinateur.

M. Robinson (Etobicoke—Lakeshore): C'est-à-dire en ce qui concerne l'admissibilité?

M. Georgas: C'est exact.

En ce qui concerne la crédibilité, à mon sens c'est quelque chose de complètement différent. Il faudrait étudier les programmes informatiques qui ont permis de manipuler les données pendant des mois et la conduite de l'organisme qui s'est servi du système informatique et peut-être la période pendant laquelle les données ont été emmagasinées dans l'ordinateur. Ces questions sont différentes, et il y en a deux.

M. Robinson (Etobicoke—Lakeshore): Je veux vous poser une dernière question qui porte sur le projet d'article 159 du Bill S-33 où l'on exclut la force probante des documents, cet article stipule:

Un document qui, en vertu d'un texte législatif autre que la présente loi fait preuve de l'existence d'un fait, établit ce fait en l'absence de preuve contraire lorsque rien dans le contexte n'indique la force probante de cette preuve.

Que pensez-vous de cet article en ce qui concerne les délits informatiques? Faudrait-il ajouter ou retrancher certaines dispositions ou l'article tel que libellé est-il satisfaisant?

M. Georgas: Pour paraphraser le projet d'article 159—veuillez me corriger si je me trompe en le lisant—il est dit que s'il existe une autre loi, les faits seront établis en l'absence de preuve contraire. Si cette loi est en vigueur, la loi sur la preuve au Canada où le Bill S-33 donnerait effet à cette disposition. Est-ce exact?

[Text]

Mr. Robinson (Etobicoke—Lakeshore): In substance I would be inclined to agree with you, that it is something that would be used.

Mr. Georgas: If you are proposing to amend the Criminal Code to that effect, that a record adduced into evidence will be given 100% credibility unless the other side can prove otherwise, I would not go that far, no. Particularly with computerized evidence, you do have to look at how the data was manipulated within the system.

Mr. Robinson (Etobicoke—Lakeshore): So you are really looking, when you are talking about the credibility of the data you are looking at, at its reliability as well?

Mr. Georgas: That is correct.

Mr. Robinson (Etobicoke—Lakeshore): Its accuracy as well?

Mr. Georgas: Correct. But that is something different from admissibility.

Mr. Robinson (Etobicoke—Lakeshore): But should the onus not be on the person presenting that piece of evidence to indicate the reliability and the credibility it should have?

Mr. Georgas: At what point in time? To get it in?

Mr. Robinson (Etobicoke—Lakeshore): To get it in.

Mr. Georgas: No.

Mr. Robinson (Etobicoke—Lakeshore): You think that is something that should be done afterwards, after it has already been admitted?

Mr. Georgas: That is correct. What he has to show—in my point of view—to get it in, is a printout, an accurate representation of what is in the machine. Then the evidence goes in. Then all the considerations as to whether what is on that printout is an accurate representation of what has happened in the course of events, goes to credibility.

Mr. Robinson (Etobicoke—Lakeshore): And it does not matter whether the information on it is accurate or not.

Mr. Georgas: From the point of view of admissibility?

Mr. Robinson (Etobicoke—Lakeshore): Yes.

Mr. Georgas: No. Thank you, Madam.

The Chairman: Maybe we will take two or three minutes. I think Mr. Beatty does not have any other questions, so I would just like to thank you for your exposé. Certainly it has given us some clarification and some help. We hope you will read our report and be able to give your comments in the future, after putting all together the information we get. We would welcome again your comments. So thank you for appearing before us.

Before I go to Mr. Tollefson, we might just take a little recess for a few minutes.

[Translation]

M. Robinson (Etobicoke—Lakeshore): J'aurais tendance à être d'accord avec vous sur le fond, c'est une disposition que l'on utiliserait.

M. Georgas: Si vous proposez de modifier le Code criminel, pour que les faits soient crédibles à 100 p. 100, à moins que l'autre partie puisse prouver le contraire, je n'irais pas jusque là. Surtout en ce qui concerne les preuves informatisées, il faut voir comment les données ont été manipulées dans le système.

M. Robinson (Etobicoke—Lakeshore): Donc en parlant de crédibilité des données, vous essayez de voir si ces données sont également fiables?

M. Georgas: C'est exact.

M. Robinson (Etobicoke—Lakeshore): Si elles sont exactes également?

M. Georgas: C'est exact, mais c'est une considération différente de l'admissibilité.

m. Robinson (Etobicoke—Lakeshore): Mais la charge de la preuve ne devrait-elle pas incomber à la personne qui présente les faits, laquelle devrait indiquer leur degré de fiabilité et de crédibilité?

M. Robinson: Quand? Pour que ces faits soient admissibles en cour?

M. Robinson (Etobicoke—Lakeshore): C'est exact.

M. Georgas: Non.

M. Robinson (Etobicoke—Lakeshore): Vous pensez que c'est quelque chose qui devrait être fait après que les faits aient déjà été admis?

M. Georgas: C'est exact. Ce qu'il doit montrer—à mon sens—c'est une imprimante, c'est-à-dire un support écrit exact des données qui se trouvent dans la machine. Après, les faits sont admissibles. Maintenant à savoir si tout ce qui figure sur cette imprimante est exactement ce qui s'est passé, cela est une question de crédibilité.

M. Robinson (Etobicoke—Lakeshore): Et peu importe si les renseignements qui figurent sur cette imprimante sont exacts ou non.

M. Georgas: Du point de vue de l'admissibilité?

M. Robinson (Etobicoke—Lakeshore): Oui.

M. Georgas: Non, merci, madame.

Le président: On pourrait peut-être faire une pause de quelques minutes. Je pense que M. Beatty n'a plus d'autres questions à poser, en conséquence permettez-moi de vous remercier pour votre exposé, qui nous apporté certaines précisions. Nous espérons que vous lirez notre rapport et que vous nous ferez part de vos réactions, lorsque nous aurons mis ensemble toutes les données que nous avons. C'est avec plaisir que nous écouterons à cette occasion ce que vous avez à nous dire. Merci d'avoir comparu aujourd'hui.

Avant de passer à M. Tollefson, nous pourrions peut-être prendre une pause de quelques minutes.

[Texte]

[Traduction]

• 1125

• 1130

Le président: La réunion se poursuit, et nous allons entendre maintenant un représentant du ministère de la Justice. Bienvenue monsieur, et merci de votre collaboration.

Peut-être pourriez-vous présenter les personnes qui vous accompagnent ce matin?

M. E.A. Tollefson (coordonnateur, ministère de la Justice): Certainement madame le président.

Mes collègues sont Me Norman Hill, Elizabeth Gilhooly et Donald Piragoff, tous les trois sont avocats au ministère de la Justice. Maintenant, si je pouvais continuer en anglais...

Le président: À votre choix.

M. Tollefson: Merci beaucoup.

As I understand it, Madam President and members of the subcommittee, I have been called to give you a résumé of the position of the Department of Justice in relation to the evidentiary aspects of the question on computers that you are dealing with.

Perhaps I should start by giving you just a very brief history of Bill S-33. As you recall, Bill S-33 is based upon the uniform evidence act which was approved by the Uniform Law Conference of Canada at its annual meeting in August of 1981. That uniform act in turn was based upon the recommendations of a federal-provincial task force on uniform rules of evidence.

I think that is the real starting point. The task force looked at the question of the admissibility of computer evidence and they came to the conclusion that it was probably desirable to have a few basic conditions of admissibility. They looked at the conditions of admissibility employed in England, in the United States, in Australia—and some that were proposed for South Africa.

You can find their recommendations in the report of the task force, which was published by Carswell, at pages 399 to 401. They recommended that there be three conditions of admissibility: first of all, proof that the data upon which the printout is based is of a type regularly supplied to the computer during the regular activities of the organization from which the printout comes; second, proof that the entries into the data base from which the printout originates were made in the regular course of business; and, third, proof that the computer program used in producing the printout reliably and accurately processes the data in the data base.

There was a great deal of discussion in the Uniform Law Conference as to whether these conditions of admissibility were in fact desirable, and the position taken by the Uniform Law Conference was that these conditions were really not necessary and that no distinction should be drawn between

The Chairman: Order, please! We shall now hear from a representative of the Department of Justice. Welcome sir and thank you for your co-operation.

You could maybe introduce the people who accompany you this morning.

Mr. E.A. Tollefson (Co-ordinator, Department of Justice): Thank you Madam Chairman.

The people who accompany me are Mr. Norman Hill, Elizabeth Gilhooly and Donald Piragoff, the three of them are lawyers working for the Department of Justice. Now with your permission I shall carry on in English.

The Chairman: It is up to you.

Mr. Tollefson: Thank you very much.

Madame la présidente, messieurs les membres du Comité, si j'ai bien compris vous m'avez demandé de comparaître aujourd'hui pour vous résumer la position du ministère de la Justice en ce qui concerne les questions de preuve relatives à votre ordre de renvoi.

Je pourrais peut-être commencer par un bref rappel des faits qui ont donné lieu au Bill S-33. Comme vous vous en souvenez, le Bill S-33 découle de la loi uniforme sur la preuve qui a été adoptée par la Conférence canadienne de l'uniformisation du droit à l'occasion de sa réunion annuelle en août 1981. Cette loi à son tour découle des recommandations qui ont été faites par un groupe d'étude fédéral-provincial chargé d'étudier l'uniformisation des règles en matière de preuves.

Voilà le point de départ. Le groupe d'étude a étudié la question de la recevabilité des faits informatisés au tribunal et on est arrivés à la conclusion qu'il était probablement souhaitable de l'assortir de quelques conditions fondamentales. Ils ont étudié les conditions de recevabilité dans le système britannique américain et australien—ainsi que certaines autres qui avaient été proposées en Afrique du sud.

Le groupe d'étude a rédigé un rapport publié par Carswell dans lequel on trouve ses recommandations, aux pages 399 à 401. Il recommande que la recevabilité des faits informatisés soit assortie de trois conditions. Premièrement, il faut prouver que les données qui figurent sur l'imprimante sont régulièrement transmises à l'ordinateur pendant les activités normales de l'organisme d'où provient l'imprimante; deuxièmement, prouver que l'accès aux bases de données d'où provient l'imprimante a été effectué normalement et troisièmement prouver que le programme informatisé dont on s'est servi pour obtenir l'imprimante reflète de façon fiable et précise les données qui se trouvent dans la banque de données.

On a beaucoup parlé à la Conférence canadienne de l'uniformisation du droit de l'opportunité de ces conditions de recevabilité, et la Conférence en est arrivée à la conclusion que ces conditions n'étaient à vrai dire pas nécessaires et qu'il n'y

[Text]

records that were kept in a computer and records that were kept in an ordinary ledger book or any other kind of business record.

The guarantee of reliability for an ordinary business record is that it is made in the usual and ordinary course of business. The fact that it is made this way and that business relies upon these documents is a sufficient guarantee of the documents' trustworthiness that the court should be prepared to accept those documents into evidence. Other questions relating to the manner in which the document was made, the control mechanisms for access to the document, other security techniques that were employed by the business all went to weight according to the Uniform Law Conference. Therefore, the Uniform Law Conference came to the conclusion that these three conditions were not necessary at all, that the same basic rules should apply to computerized documentation as applied to other business records and all you had to do was to show that the original itself was reasonably reliable.

• 1135

I would draw to your attention the fact that the reference to the Uniform Evidence Act made by Mr. Georgas is in fact incorrect. He referred, I think, to Section 171, and I am sorry to say he was looking at an earlier draft, and not the draft that was approved by the Uniform Law Conference of Canada itself. The Uniform Evidence Act, Section 130, made the following provision as far as an original is concerned. It simply said:

(c) in relation to stored or processed data or information, any printout or intelligible output shown to reflect accurately the data or information . . .

There is no other provision relating to computer evidence at all in the Uniform Evidence Act. They said that they did not need it. Just apply the ordinary business documents' rules, and for definition of an original, look at the definition in Section 130, which, and I will repeat it, says:

(c) in relation to stored or processed data or information, any printout or intelligible output shown to reflect accurately the data or information . . .

Mr. Robinson (Etobicoke—Lakeshore): That is not, if I may interject, the definition of original, as contained in this Bill S-33.

Mr. Tollefson: No. That is quite so. I was just going to explain why the department did not follow that definition.

Following the approval of the Uniform Evidence Act, it was drawn to our attention that this could impose a very heavy burden upon the proponent of computerized documents, because how do you show that this printout reflects accurately the data or information? Do you have to call, as they required in the McMullen case in the Ontario Court of Appeal, witnesses for every aspect of the system to show that the system in fact does reproduce accurately the material that was input . . . the original information?

[Translation]

avait donc pas lieu d'établir une distinction entre les dossiers informatisés et tout autre dossier d'affaires ou livre comptable.

La garantie de fiabilité pour tout dossier d'affaires ordinaires réside dans le fait que ces dossiers sont généralement constitués au fur et à mesure des transactions commerciales. Le fait qu'ils soient constitués de cette façon est que les compagnies se fient sur ces documents est une garantie suffisante quant à leur fiabilité pour que les tribunaux les tiennent pour recevables en tant que preuves. La Conférence a également pris en compte d'autres questions relatives à la façon dont les documents ont été élaborés, les mécanismes de contrôle relatifs à l'accès aux documents ainsi que d'autres techniques en matière de sécurité utilisées par les compagnies. En conséquence, la Conférence en est arrivée à la conclusion que ces trois conditions n'étaient pas nécessaires du tout, et que les mêmes règles fondamentales s'appliquaient à tous les documents, informatisés ou non, et que la seule preuve à faire consistait à prouver que l'original était raisonnablement fiable.

Je voudrais attirer votre attention sur le fait que ce que M. Georgas a dit au sujet de la Loi uniforme sur la preuve, est inexact. Il a parlé, je pense, de l'article 171 et je regrette de devoir dire qu'il a cité un projet de loi antérieur et pas celui qui a été approuvé par la Conférence canadienne de l'uniformisation du droit. L'article 130 de la Loi uniforme sur la preuve parlait en ces termes d'un original:

3. Lorsqu'il concerne des données informatisées, tout document intelligible provenant de l'appareil où elles sont emmagasinées et les reflétant fidèlement . . .

Il n'y a aucune autre disposition relative aux faits informatisés dans la Loi uniforme sur la preuve. On ne les a pas jugés nécessaires. Il s'agit tout simplement d'appliquer les règles ordinaires en matière de documents d'affaires et pour la définition d'original, de jeter un coup d'oeil à la définition qu'on en donne à l'article 130 que je vais répéter:

3. . . . lorsqu'il concerne des données informatisées tout document intelligible provenant de l'appareil où elles sont emmagasinées et les reflétant fidèlement . . .

M. Robinson (Etobicoke—Lakeshore): Si vous me permettez de vous couper la parole, ce n'est pas la définition d'original que l'on trouve dans le Bill S-33.

M. Tollefson: Non, c'est tout à fait exact. J'allais vous expliquer pourquoi le ministère n'a pas suivi cette définition.

Après l'approbation de la Loi uniforme sur la preuve, on a attiré notre attention sur le fait que cela pourrait rendre beaucoup plus difficile pour ceux qui sont en faveur de l'informatisation des documents, de prouver que telle imprimante reflète exactement telle donnée ou tel renseignement, ce qui n'est pas très commode? Pour cela, faut-il comme cela a été le cas dans l'affaire McMullen portée devant la Cour d'appel de l'Ontario, citer des témoins à comparaître pour chaque aspect du système afin de prouver que le système a

[Texte]

So the Department said, let us modify this bit, make it a bit easier for the proponent. There should be in fact two different ways in which the data can be proven to be an original. So it now reads in Clause 130 of Bil S-33:

(c) in relation to stored or processed data or information, any printout or intelligible output that reflects accurately the data or information . . .

That is essentially the same as what the Uniform Evidence Act said:

. . . or is the product of a system that does so.

Now, we could foresee two different ways, in other words, of showing that the printout was in fact sufficiently reliable to be admitted as an original. This has happened rarely, but it could happen: the original document had been compared with the printout, so you just eyeballed the two of them and a witness could say, I made a comparison, the printout accurately represents or reflects what was in the original. The other is by showing that the printout is in fact the product of a system which accurately reproduces the information that is put into a system. We assume that this would mean that the proponent of the document would probably adduce by affidavit . . . this is provided for in Section 155.(2) of Bill S-33—would provide an affidavit that indicated that the system was a certain kind of system; that it was an extremely reliable system and had been place for a number of months or years. There were no problems in the system on that particular day.

• 1140

There was no indication that the document in question contained any flaws in it, and this sort of documentation, or supporting documentation, could be provided by the custodian, or some other informed witness, and the court on that basis would say: You have passed the threshold of admissibility; from now on it becomes a question of weight.

We did not think that was a particularly difficult task for a bank or for a trust company or any other major business to satisfy. On the other hand, we felt it was necessary to have some form of protection so that the court was not going to be flooded with print-outs that had to be presumed in all cases to be authentic, to be a proper representation of the original, and to be reliable.

So Bill S-33 I think is a compromise between the position taken by the people who say that no computerized evidence should be admitted unless it can be proven to be 100% reliable and the position taken by those who say: Let it in, the computer is a basically reliable tool, everything should be admitted from a computer, everything just goes to weight.

So that is the history of the provision in S-33.

In the Senate the clause has been challenged by, to date at any rate, only one organization, and that is the Canadian

[Traduction]

reproduit exactement les données qui ont été encodées—c'est-à-dire l'information originale.

En conséquence, le ministère s'est dit qu'il fallait apporter certaines modifications, pour rendre la chose un peu plus facile. Il fallait en fait qu'il existe deux façons de prouver que les données figurant sur une imprimante sont bien des originaux. En conséquence, l'article 130 du Bill S-33 stipule:

(c) relativement à des données informatisées, tout document intelligible provenant de l'appareil où elles sont emmagasinées et qui le reflète fidèlement . . .

Dans l'ensemble cette disposition est la même que celle qui figure dans la Loi uniforme sur la preuve qui stipule:

. . . ou qui est le produit d'un système qui donne le même résultat.

En d'autres termes, nous pourrions prévoir deux façons différentes de montrer qu'une imprimante était en fait suffisamment fiable pour être reçue en tant qu'original. Cela est arrivé rarement, mais cela pourrait arriver. Le document original avait été comparé à l'imprimante, donc en regardant les deux un témoin pourrait dire, j'ai comparé, et l'imprimante représente exactement ce qui était dans l'original. L'autre consiste à montrer que l'imprimante est en fait le produit d'un système qui représente exactement l'information encodée dans un système. Nous partons de l'hypothèse que cela signifierait qu'une personne devrait déclarer sous serment ce qui est prévu au paragraphe 155.(2) du Bill S-33 que le système était un certain type de système extrêmement fiable et utilisé depuis plusieurs mois ou plusieurs années. En outre, que pendant cette journée le système avait bien fonctionné.

Rien n'indiquait que le document en question contenait des vices, et ce genre de documentation, ou de documentation à l'appui, pourrait être fournie par le conservateur ou par un autre témoin informé, et le tribunal pourrait dire, en se basant là-dessus: vous avez franchi le seuil d'admissibilité; à partir de maintenant, cela devient une question de poids.

Cela ne nous paraissait pas une condition difficile à remplir pour une banque, pour une société de fiducie, ou pour toute autre grande entreprise. D'autre part, il nous paraissait nécessaire de prévoir l'une ou l'autre forme de protection, de sorte que le tribunal ne soit pas inondé d'imprimés d'ordinateur qui devaient être considérés authentiques dans tous les cas, viables et copie conforme de l'original.

Le Bill S-33 constitue donc, je pense, un compromis entre la position adoptée par ceux qui disent qu'il ne faudrait admettre aucune preuve informatisée, à moins que sa fiabilité à 100 p. 100 puisse être prouvée, et la position adoptée par ceux qui disent; admettons cette forme de preuve, l'ordinateur est un outil essentiellement fiable, tout ce qui en sort devrait être admis, tout contribue à la plausibilité de la preuve.

Telle est donc l'histoire de la disposition du Bill S-33.

Au Sénat, une seule organisation, à ce jour du moins, a récusé cette clause: il s'agit de l'Association des banquiers

[Text]

Bankers' Association. They challenged the clause on two bases essentially.

First of all, they felt the clause was not sufficiently precise with respect to the kind of foundation evidence that was going to be necessary in order to establish that the system was a system that reliably reproduced or reliably reflected the information in the original document. They are concerned still that they might be in the situation that they are left in as a result of the McMullen case; that they will have to call a large number of witnesses, witnesses who can testify to the various components of their computer system. So there is an inconvenience factor to them.

Second, they are concerned about the security element. They are afraid that if they have to divulge the different kinds of security precautions that are taken and the different kinds of programming steps that are taken to assure the reliability of the system, somehow or other this will tell the very sophisticated computer crooks that are going to be coming forward in future years how they can get into the system and perhaps either destroy their information or subtract large amounts of money from customers' accounts.

So the Canadian Bar Association, or rather the Canadian Bankers' Association . . . CBA is the initial for both of them, I get them confused from time to time . . . takes the view that we ought to be a bit more precise. I think that is their view, although they have not drafted any substitute clause for us; that we ought to be a bit more precise in terms of the nature of the foundation evidence, and it ought to be made very plain that the local accountant or bank manager can give this information to the court, or some central individual, say in their head office, can just file a certificate saying that this is an ordinary banking document and it should therefore be admitted as being a reliable document.

The Senate committee asked the representatives of the Canadian Bankers' Association to develop a new clause that the committee could consider. As far as I know, no reply has been made yet, but the Canadian Bankers' Association did indicate that they would be quite happy to attempt to do this.

• 1145

There is one other group, as I understand it, which is making a similar pitch. That is the Canadian Payments Association, and they are to appear before the Senate committee next week. I have not yet seen the brief they have submitted to the Senate; therefore I am afraid I cannot be very helpful to you. I understand that Mrs. Hébert has a copy of their brief, and I suppose that can be made available to you that way.

As far as the Department of Justice is concerned, we are not absolutely married to the wording of proposed Section 130 of Bill S-33. We are trying to come up with a provision that will satisfy the convenience of the business community, since there is obviously a very heavy burden upon the business community

[Translation]

canadiens, et ceci en se fondant essentiellement sur deux arguments.

Tout d'abord, l'association considère que la clause n'est pas suffisamment précise en ce qui concerne le genre de fondements de preuve qui seront nécessaires pour établir que le système reproduisait fidèlement ou retransmettait fidèlement l'information du document original. L'association craint de se trouver dans la situation qui découle de l'affaire McMullen, à savoir qu'il faudra faire appel à un grand nombre de témoins, témoins qui seront en mesure de déposer sur les différents éléments constituant leur système d'ordinateur. Leurs arguments se fondent donc sur la difficulté d'application de cette clause.

Le second facteur qui explique leur opposition est l'élément de sécurité. L'association craint que s'il faut divulguer les différentes catégories de précautions qui sont prises et les différentes démarches de programmation pour assurer la fiabilité du système, ces renseignements ne parviennent, de l'une ou l'autre façon, à l'escroc d'ordinateur très sophistiqué que l'avenir ne manquera pas de produire, et lui permettent de pénétrer le système, et peut-être de détruire l'information, ou de soustraire de grandes sommes d'argent des comptes des clients.

C'est pourquoi l'Association du barreau canadien, ou plutôt l'Association des banquiers canadiens—les deux associations ont le même sigle, c'est pourquoi je m'y trompe parfois—considère que nous devrions être un peu plus précis. C'est du moins ce que je crois qu'elle pense, car elle n'a pas rédigé de clause de rechange à notre intention; elle pense donc que nous devrions être un peu plus précis sur la nature des fondements de la preuve, et qu'il devrait être dit clairement que le comptable local, ou le directeur de banque, peut apporter ces informations au tribunal, ou les donner à une personnalité importante, par exemple au siège social, et peut déposer un certificat disant qu'il s'agit là d'un document bancaire ordinaire qui devrait donc être reconnu comme document digne de foi.

Le comité du Sénat a demandé aux représentants de l'Association des banquiers canadiens de rédiger une nouvelle clause qui serait mise à l'étude par le comité. Aucune réponse n'a encore été donnée, à ma connaissance, mais l'Association des banquiers canadiens a fait savoir qu'elle allait se mettre à l'ouvrage.

Je crois savoir qu'il existe un autre groupe dont les efforts vont dans le même sens, c'est la *Canadian Payments Association*, association qui doit comparaître la semaine prochaine devant le comité du Sénat. Je n'ai pas encore vu le mémoire qu'elle a présenté au Sénat, et c'est pourquoi je ne puis vous être de grande utilité. Je crois savoir que M^{me} Hébert en a un exemplaire, et qu'il sera ainsi possible de mettre le mémoire à votre disposition.

En ce qui concerne le ministère de la Justice, nous ne tenons pas à tout prix au libellé du projet d'article 130 du Bill S-33. Nous essayons de proposer une disposition qui n'accordera pas trop les milieux d'affaires, car ces derniers sont considérablement gênés par la nécessité de conserver les documents

[Texte]

in terms of keeping original records, and we do not think it is absolutely necessary that they keep these records. So we are trying to come up with a provision that will be in keeping with modern record processing systems and record retention systems which are employed.

But you have to balance that interest against the protection of the individual against whom these documents may be used. And here of course, as you are well aware, it is extremely difficult for an individual to challenge the contents of a computer printout. There is no paper trail that you can follow up. It is not easy to comprehend the printout, sometimes. Neither is it possible to comprehend, if you are just an ordinary person, the program or even the machinery that is used in processing the information.

So what we are trying to do is to achieve this balance, and we are quite prepared to look at any other formulations which will do the job better than Clause 130 of Bill S-33.

If I could just speak to one question that was addressed by Mr. Robinson to Mr. Georgas, he was asking about proposed Section 159 and the meaning of that. Proposed Section 159 is actually taken directly from the Interpretation Act. In other words, it is the law of the day. What it does basically is to say that where a document or a record is made admissible by some other act than the Canada Evidence Act, and there is no indication as to what kind of weight should be given to it, it should be taken as establishing, *prima facie*, the contents of that document. And that, of course, is not a very difficult burden to overcome.

The person who opposes that document, I presume, can overcome the effect of this *prima facie* presumption by producing some credible evidence which tends to establish that the presumption ought not to apply.

What would that apply to? Well, for example, if it is not a business record, if it is not a record that is kept in the usual and ordinary course of business but, nevertheless, some statute says that a certificate shall be prepared and the certificate shall be admissible in evidence, then you would have to ask yourself what the effect is of this certificate. And all that 159 says is that in the absence of any other indication, the effect of that certificate—because it has been identified in the statute—is admissible; that it establishes the contents of the certificate unless there is some other evidence which destroys the presumptive effect of the certificate. We felt that particular provision, being an evidentiary provision, properly belonged in an evidence act rather than an interpretation act and that is why it appears there.

If you have any questions, I will be delighted to try to answer them.

The Chairman: Mr. Beatty.

Mr. Beatty: Thank you very much, Madam Chairman.

Thank you for a very helpful presentation. It was very lucid and very useful, I think, to the committee, because it is the one

[Traduction]

originaux, et il ne nous paraît pas indispensable qu'ils le fassent. Nous essayons donc d'introduire une disposition qui répondra aux besoins des systèmes modernes de traitement et d'archivage des documents.

Mais il faut également tenir compte, en regard de cet intérêt, de la protection de l'individu contre lequel ces documents peuvent être utilisés. Et vous n'ignorez certainement pas qu'il est très difficile à une personne de récuser le contenu d'un imprimé d'ordinateur. Il n'est pas possible de demander à voir les pièces du dossier. Il n'est parfois pas facile de comprendre l'imprimé d'ordinateur. Et si vous êtes un simple particulier, il n'est pas non plus possible de comprendre le programme, voire l'équipement utilisé pour le traitement de l'information.

Nous essayons donc de parvenir à équilibrer ces deux facteurs, et nous sommes tout à fait disposés à étudier tout autre libellé qui serait plus satisfaisant que l'article 130 du Bill S-33.

Permettez-moi également de commenter une question adressée à M. Georgas par M. Robinson, qui posait des questions sur le projet d'article 159 et sur sa signification. Ce projet d'article 159 est tiré directement de la Loi d'interprétation, autrement dit, c'est la loi actuelle. Cette loi stipule, pour l'essentiel, que lorsqu'un document ou une archive est recevable en vertu d'une loi autre que la Loi sur la preuve au Canada, et qu'il n'existe pas d'indications sur le genre de poids à lui donner, il conviendrait de considérer ce document comme ayant force probante. Ce qui, bien entendu, ne pose pas de grandes difficultés.

La personne qui fait opposition à ce document peut, j'imagine, surmonter l'obstacle de ce commencement de preuve en produisant une preuve crédible tendant à invalider la présomption.

A quoi cette situation s'appliquerait-elle? Par exemple, s'il ne s'agit pas d'archives commerciales, ou d'un document qu'il est d'usage de conserver, dès qu'une loi stipule, néanmoins, qu'il convient de préparer un certificat et que ce certificat constituera une preuve recevable, il faut se demander ce que sera l'effet de ce certificat. Tout ce que dit l'article 159, c'est qu'en l'absence de toute autre indication, l'effet de ce certificat, puisqu'il a été identifié par la loi, est recevable, qu'il établit la teneur du certificat, à moins qu'il n'existe une autre preuve qui va à l'encontre de l'effet de présomption du certificat. Nous avons jugé que cette disposition particulière, établie pour constituer la preuve, devrait trouver sa place dans une loi sur la preuve plutôt que dans une loi d'interprétation, et c'est pourquoi elle figure ici.

Si vous avez des questions à poser, je serai heureux d'essayer d'y répondre.

Le président: Monsieur Beatty.

M. Beatty: Je vous remercie beaucoup, madame le président.

Votre exposé a été très clair et très utile à ce comité, je crois, car c'est un domaine sur lequel nous ne nous sommes pas

[Text]

area in our inquiry to which we have not directed a great deal of attention so far, but one which is obviously important.

• 1150

The first thing that comes to mind, to me, is that I guess one should not legislate unless one has to. You presumably have looked at all of the current case law. Is there, in fact, a need to amend the Canada Evidence Act at this point, particularly after *R. v. Bell and Bruce*?

Mr. Tollefson: I am speaking now in terms of the Uniform Law Conference of Canada and the Department of Justice. The position taken by all the governments that are represented in the Uniform Law Conference of Canada and our own department is that there is some need for clarification but we do not need to go into great detail. We think we can accomplish the same objectives by applying general evidentiary provisions, particularly to defining the term "original", defining the term "duplicate", in a broad sense so that the kinds of records that are kept, whether they are produced by computer or produced by some other means that guarantees an accurate reproduction, for example a Xerox copy, should be admissible.

Mr. Beatty: As regards computer printouts, though, what problems were left undealt with by *R. v. Bell and Bruce*?

Mr. Tollefson: I would like to look at Bell and Bruce again before I answer you finally, but I think the question of the definition of what is an original perhaps was not clearly set out in Bell and Bruce. My recollection is that Bell and Bruce said that if you did not have the original, if it was no longer in existence and the bank relied upon the printout as if it were the original, that meant that you could treat it as an original. Suppose you do not, in fact, have that kind of factual situation; it seems to me that you may want to have a definition of original that includes a computer printout, if the computer printout can be shown to be the product of a program that reliably reproduces information. That, I think, would be my answer for that.

Mr. Beatty: I was just taking a look at Mr. Justice Weather-
spoon's opinion on Fairweather's decision and he certainly makes the point that the printout may become the original record in time.

Mr. Tollefson: He does not say, however, that it always has to be treated as an original, as I understand it.

Mr. Beatty: No, but it certainly does not rule that out either, I suppose. What I am wondering is whether we are not finding an evolution in the law, or a flushing out of the law, in the courts themselves that is solving this problem by itself without legislative changes by Parliament.

Mr. Tollefson: I think that is entirely possible. I think many of the fears that the business community had, or the banking community in particular had, as a result of the McMullen case have proven to be groundless. I have not seen any great flood

[Translation]

encore beaucoup penchés jusqu'à présent, et qui est, de toute évidence, très important, et je vous en remercie.

La première chose qui me vient à l'esprit, c'est que je crois qu'on ne devrait pas légiférer à moins qu'on y soit obligé. Vous avez probablement étudié toute la jurisprudence actuelle. Est-il en fait besoin de modifier maintenant la Loi sur la preuve au Canada, en particulier après l'affaire *R. c. Bell and Bruce*?

M. Tollefson: Je parle maintenant du point de vue de la Conférence canadienne de l'uniformisation du droit et du ministère de la Justice. La position adoptée par tous les gouvernements représentés à cette conférence et par notre propre ministère, c'est qu'il est nécessaire de préciser certaines choses, mais sans trop entrer dans les détails. Nous pensons pouvoir atteindre les mêmes objectifs en appliquant des dispositions générales concernant la preuve, en particulier en définissant les termes «original» et «double» dans un sens large, de sorte que le genre de documents conservés, qu'ils soient produits par ordinateur ou par tout autre moyen garantissant une reproduction fidèle, par exemple une photocopie, devraient être recevables.

M. Beatty: En ce qui concerne les imprimés d'ordinateur, quels étaient les problèmes qui n'avaient pas été traités dans l'affaire *R. c. Bell and Bruce*?

M. Tollefson: Avant de pouvoir vous donner une réponse définitive, j'aimerais consulter le dossier *Bell and Bruce*, mais je crois que dans l'affaire *Bell and Bruce*, il n'y avait pas eu de définition claire de ce en quoi consiste un original. Je crois me souvenir qu'on y disait que si vous n'avez pas l'original, s'il n'existait plus et si la banque devait se fier à un imprimé d'ordinateur comme s'il s'agissait de l'original, cela signifiait que vous pouviez traiter cet imprimé comme s'il s'agissait de l'original. Mais supposons que vous ne vous trouviez pas, en fait, dans ce genre de situation de fait, il me semble que vous voudriez avoir une définition qui comprenne également, comme original, un imprimé d'ordinateur, s'il peut être prouvé que cet imprimé est le produit d'un programme qui reproduit fidèlement une information. Ceci, à mon avis, constituerait ma réponse à cette question.

M. Beatty: Je viens justement de prendre connaissance de l'opinion du juge Weatherspoon sur la décision de Fairweather, et il établit certainement que l'imprimé d'ordinateur est susceptible de constituer l'original à un certain moment.

M. Tollefson: Il ne dit toutefois pas qu'il convient toujours de le traiter comme un original, si j'ai bien compris.

M. Beatty: Non, mais il ne l'exclut pas non plus, à mon avis. Je me demande si nous ne pouvons pas constater une évolution du droit, si devant les tribunaux même on n'écarte pas le droit, pour résoudre en soi ce problème sans intervention législative du Parlement.

M. Tollefson: C'est fort possible. Nombre des craintes éprouvées par les milieux d'affaires ou les milieux bancaires en particulier, à la suite de l'affaire McMullen, se sont avérées sans fondement. Nous n'avons pas été inondés de cas où les

[Texte]

of cases where the banks have great difficulty in establishing the records that were produced.

Mr. Beatty: The evidentiary provisions in my bill were as a result of concerns arising out of MacMillan, since that time that *R. v. Bell and Bruce* was brought to my attention.

Mr. Robinson (Etobicoke—Lakeshore): Has that been appealed yet?

Mr. Beatty: That was an appeal.

Mr. Tollefson: I do not know whether there was an appeal to the Supreme Court of Canada. Certainly there was none in . . .

Mr. Robinson (Etobicoke—Lakeshore): There was a new trial ordered.

Mr. Beatty: But the decision was certainly made by the Supreme Court of Ontario, as related to the admissibility of the printout.

I guess you hear two major concerns that are expressed about the need to have someone testify as to the authenticity of the record and of the process that is followed there. The first is that it may be costly and involve a great deal of time for senior executives. I do not have a great deal of sympathy there. If a person is taken to court and accused of a very serious offence, it seems to me that it is not a very valid argument to make that somebody is too important to be bothered coming to court to testify. The other, which you put your finger on, is of concern to the Canadian Bankers' Association. Its concern is that this sort of testimony could disclose the procedures used to ensure security. I can see that would be a very real concern.

• 1155

But how would that differ from a case where, for example, under trade secrets legislation, it was necessary to establish that something was, in fact, a secret? My understanding of trade secrets legislation is that to establish that, in fact, a secret has been improperly broken in some way or revealed in some way, you have to establish the methods you took to keep it a secret. Conceivably, could you not run into the same problems under trade secrets legislation as under this sort of testimony? It may be inconvenient for the individual or for the organization involved, but it is not a radical new departure.

Mr. Tollefson: I think you are quite right in your assumption that there is an analogy to be drawn. I would agree with you that in a very serious case where a person's liberty may very well be involved, the financial institutions should not necessarily be able to hide behind the corporate veil, so to speak, and say: Well, this information is obviously reliable; if we rely on it, that should be good enough for you.

Mr. Beatty: I suppose the case of the Official Secrets Act would be somewhat different. The Crown would not have to go

[Traduction]

banques ont eu des difficultés considérables à faire la preuve avec les documents qu'elles produisaient.

M. Beatty: Les dispositions de mon projet de loi qui portent sur la preuve sont l'aboutissement des préoccupations soulevées par l'affaire MacMillan, depuis l'époque où l'affaire *R. c. Bell and Bruce* a été portée à mon attention.

M. Robinson (Etobicoke—Lakeshore): Est-ce qu'on a interjeté appel?

M. Beatty: C'était en appel.

M. Tollefson: Je ne sais pas si on a interjeté appel auprès de la Cour suprême du Canada. Il n'y en avait certainement pas dans . . .

M. Robinson (Etobicoke—Lakeshore): On a rouvert le procès.

M. Beatty: Mais la Cour suprême de l'Ontario a certainement pris la décision concernant la recevabilité de l'imprimé d'ordinateur.

Deux objections principales sont mises en avant sur la nécessité de faire témoigner quelqu'un sur l'authenticité du document et le processus qui est ainsi suivi. La première, c'est que c'est un processus onéreux et qui prend beaucoup de temps aux cadres supérieurs de l'entreprise. Cet argument ne me paraît pas très probant. Si une personne doit comparaître au tribunal et être accusée d'un délit très grave, dire qu'une personne est trop importante pour qu'on l'importune en lui demandant de témoigner au tribunal ne me paraît pas un argument très valide. L'autre objection, que vous touchez du doigt, a été mise en avant par l'Association des banquiers canadiens, qui craint que ce genre de témoignage ne divulgue les procédures utilisées pour assurer la sécurité. Je comprends que ceci inspire de graves inquiétudes.

Mais en quoi un tel cas différerait-il d'un autre où, par exemple, aux termes d'une loi sur les secrets de fabrication, il serait nécessaire d'établir que quelque chose constituait en fait un secret. D'après ce que je sais de la loi sur les secrets de fabrication, pour établir qu'un secret a été violé ou divulgué de l'une ou l'autre façon, il faut exposer les méthodes employées pour garder ces procédés de fabrication secrets. Ne serait-il donc pas possible de se heurter au même genre de difficultés, aux termes de la loi sur les secrets de fabrication, que pour ce genre de témoignage? C'est peut-être inconfortable pour la personne ou pour l'organisation en question, mais cela ne constitue pas un cas totalement différent.

M. Tollefson: Vous avez tout à fait raison, je crois, d'y voir une analogie. Dans un cas très grave où la liberté d'une personne est peut-être en jeu, je pense, comme vous, que les institutions financières ne devraient pas nécessairement chercher refuge dans le secret professionnel, pour ainsi dire, en disant: cette information est fiable, de toute évidence; si nous nous y fions, nous, vous n'avez aucune raison d'avoir des doutes.

M. Beatty: Je pense que le cas de la Loi sur les secrets officiels serait légèrement différent. La Couronne n'aurait

[Text]

to any pains to establish the extent to which it went to keep an official secret a secret. The mere fact that a classification makes it an official secret is enough. Or am I wrong on that?

A Witness: I am not certain of that.

Mr. Beatty: Maybe Mr. Hill might be able to clarify that.

What I was getting at was this. I was wondering if it might be a different case with the Official Secrets Act, that it might not be necessary to testify how an official secret is kept a secret; but rather, the mere classification of a secret as an official secret would be enough to have it designated.

Mr. Norman Hill (Department of Justice): I would think so. That would be the intent of the law, in any event; and of course, there is the power to have in camera hearings where those matters are concerned.

Mr. Beatty: Would there be other instances either of you could think of where an institution might be forced to disclose the security measures they had taken to protect information in court, other than trade secrets legislation? I suppose you might find some instances where contracts were involved, too.

Mr. Tollefson: Hospital documentation, I think, would be another example; the records of a patient, the treatment that is provided and this kind of thing. Obviously, the hospital wants to protect the patient from any invidious comment that may be made as to the nature of his illness and so forth. I am sure you have had this kind of representation before you.

Mr. Beatty: What about the Bank Act? I believe The Canadian Bankers' Association, when they were before us, said there are provisions within the Bank Act dealing with security standards.

Mr. Tollefson: I am not sure of that, I am sorry. I am out of my field.

Mr. Beatty: In the case of an alleged breach of the Bank Act, you might very well find testimony given as to the bank's security standards. Does Mr. Hill know, possibly?

Mr. Hill: There are provisions. I cannot visualize a case in which the security measures themselves may be the subject of the inquiry.

Mr. Beatty: What occasioned the question, Mr. Hill, was that—I think you were doing research at the time I asked it—it was pointed out that The Canadian Bankers' Association expressed a concern about the provisions in Bill S-33 in that they could require the disclosure of the measures taken to protect information by the banks. I gather their argument is that it might make it easier, subsequently, for someone to break security if this information were disclosed. I can certainly understand that concern, but it seems to me that, likely, the problem is not a particularly novel one.

Mr. Hill: I would think Bill S-33 is dealing more with the accuracy of the records rather than the measures taken to protect the information in the bank; in other words, the system itself, the integrity of the system, the reliability of the way in

[Translation]

aucune difficulté à établir jusqu'où elle est allée pour conserver le secret sur une question. Le seul fait de classer une question comme secrète est suffisant. C'est bien cela, n'est-ce pas?

Un témoin: Je n'en suis pas sûr.

M. Beatty: M. Hill pourra peut-être tirer cela au clair.

Voici où je voulais en venir: je me demandais si la situation serait différente avec la Loi sur les secrets officiels, car il ne serait pas nécessaire de témoigner pour expliquer comment un secret officiel reste secret, et il suffirait qu'il ait été classé secret.

M. Norman Hill (ministère de la Justice): Oui, c'est bien ce que je pense. Ce serait l'intention de la loi, de toute façon, et lorsqu'il s'agit de questions de ce genre, l'audition de témoins peut se faire à huis clos.

M. Beatty: Pouvez-vous penser à d'autres cas où une institution serait obligée de divulguer au tribunal les mesures de sécurité qu'elle a prises pour protéger l'information, dans des cas autres que la loi sur les secrets de fabrication? Vous pourriez également trouver des cas où il s'agit de contrats, j'imagine.

M. Tollefson: La documentation hospitalière constituerait un autre cas, je pense; le dossier du patient, le traitement qu'il a reçu, et ce genre de renseignements. L'hôpital veut, de toute évidence, protéger le malade de tout commentaire déplaisant quant à la nature de sa maladie, et autres considérations. Je suis sûr que ce genre de cas vous a été exposé.

M. Beatty: Qu'en est-il de la Loi sur les banques? Je crois que l'Association des banquiers canadiens, lorsqu'elle a comparu devant nous, a déclaré qu'il existait dans cette loi des dispositions traitant des normes de sécurité.

M. Tollefson: Je n'en suis pas sûr, je regrette. Ceci n'est plus de ma spécialité.

M. Beatty: Dans le cas d'une infraction présumée à la Loi sur les banques, il est fort possible qu'il y ait des témoignages sur les normes de sécurité bancaire. M. Hill serait-il au courant?

M. Hill: Il existe des dispositions. Je ne puis me souvenir d'un cas précis où les mesures de sécurité elles-mêmes ont fait l'objet d'enquête.

M. Beatty: Ce qui m'a amené à poser cette question, monsieur Hill, c'est que—je crois que vous faisiez de la recherche à l'époque où j'ai posé la question—on a mentionné que l'Association des banquiers canadiens a exprimé des inquiétudes sur les dispositions du projet de loi S-33 qui exigeraient la divulgation des mesures prises par les banques pour protéger l'information. L'argument de l'association, c'est que si cette information est divulguée, il serait plus facile de tourner les mesures de sécurité. Je comprends cette préoccupation, mais il me semble fort probable que le problème n'est pas neuf.

M. Hill: Je crois que le projet de loi S-33 traite davantage de l'exactitude des archives plutôt que des mesures prises par la banque pour protéger l'information; autrement dit, c'est plutôt du système lui-même qu'il s'agit, de son intégrité, de la

[Texte]

which the records are kept up to the point of time when they are inputted into the computer and measures of that sort. I do not think it could be reasonably argued that that bill, or any provision of that bill, requires the security arrangements to be canvassed as a means of ensuring the admissibility of any records.

• 1200

Mr. Beatty: Did I misunderstand the concern of the Canadian Bankers' Association?

Mr. Tollefson: No, I think their concern is certainly in relation to security and I can see how, for example, security may very well affect the reliability of the information. If the security is lax and all sorts of people have access to the information, there is always the possibility of tampering or some modification of the information. Therefore, certainly if Mr. Chase had been here today, he would have made a very strong point of the fact that unless you can establish that nothing has happened to the information between the time of input and the time it is produced, in terms of the printout produced by the court—unless you can establish that, you have nothing and you would say that the printout ought to be excluded.

Now, I think that really it is something that should go more to weight than to admissibility, but if you can establish that your system generally—I pick up where Mr. Georgas has left off—if you can establish that your system generally produces information, produces a printout that is reliable, that should be enough to get you over the admissibility threshold, and after that there should be some obligation on the person who opposes the document to challenge it and to raise doubts as to the validity or reliability of the document based on whatever the way the records were kept, the time between the moment when the information was generated and when it was recorded, the way in which it was massaged by the program, the kind of security methods that were in place in order to protect the integrity of the information in the system itself. I think that in terms of admissibility, if that is what we are concerned with, you should be able to get in the information simply by showing that the system is generally very reliable.

Mr. Beatty: One last area I want to touch on; in your oral presentation, you put your finger on what I think is a very serious problem and that is the credibility—the extremely high credibility of computerized records. I think each one of us is susceptible to according a greater credibility to something we receive that is spewed out by a computer as opposed to something that is handwritten. For example, I know in my own case, notwithstanding the fact that I know better, I do not closely check my credit card statements I get each month. I assume it is because of the credibility of the computer printout that I get. Yet each of us knows it is every bit as easy to have an error made on those statements as it would be on any other.

One of the concerns I suppose I have with the admissibility of computerized printouts in evidence is the effect upon the rights of the accused, because of the very credibility of the

[Traduction]

fiabilité de l'archivage jusqu'au moment où les données sont introduites dans l'ordinateur, et des mesures de cet ordre. Je ne pense pas qu'il puisse être raisonnablement proposé que ce projet de loi, ou toute disposition de ce projet de loi, dise qu'il faille discuter à fond des dispositions de sécurité pour assurer que les documents soient recevables.

M. Beatty: Aurais-je donc mal compris l'Association des banquiers canadiens?

M. Tollefson: Non, l'association se préoccupe certainement de la sécurité, et j'imagine fort bien comment la sécurité pourrait, par exemple, porter atteinte à la fiabilité de l'information. Si la sécurité est relâchée, et si toutes sortes de personnes ont accès à l'information, il existe toujours une possibilité de trafiquer l'information ou de l'altérer. C'est pourquoi, si M. Chase avait été ici aujourd'hui, il aurait certainement insisté vigoureusement sur le fait que si vous ne pouvez prouver qu'il n'a pas été touché à l'information entre le moment où elle est introduite dans l'ordinateur et le moment où elle en sort, sous forme d'imprimés d'ordinateur présentés au tribunal—si vous ne pouvez donc prouver cela, votre preuve est sans fondement, et on peut arguer que l'imprimé devrait être exclu.

Je pense vraiment que ceci relève davantage du poids de la preuve que de sa recevabilité, mais si vous pouvez établir votre système, d'une façon générale—je reprends le fil de ce que disait M. Georgas—si vous pouvez donc établir que votre système produit de l'information, produit un imprimé qui est fiable, ceci devrait suffire pour vous faire franchir le seuil de recevabilité, et à partir de ce moment-là, la personne qui s'oppose au document devrait avoir l'obligation de le récuser et d'élever des doutes sur la validité ou la fiabilité du document, en invoquant la façon dont les archives sont conservées, le temps qui s'est écoulé entre le moment où l'information a pris naissance et le moment où elle a été enregistrée, la façon dont elle a été reprise par le programme, les méthodes de sécurité mises en place pour protéger l'intégrité de l'information dans le système même. En termes de recevabilité, si c'est ce dont nous nous préoccupons, vous devriez pouvoir faire passer l'information en montrant, tout simplement, que le système, d'une façon générale, est très fiable.

M. Beatty: Il y a une dernière question que je voudrais aborder: dans votre exposé, vous avez mis le doigt sur ce qui me paraît un problème très grave, à savoir la crédibilité—le haut niveau de crédibilité des archives informatisées. Chacun d'entre nous a tendance, je crois, à se fier davantage à ce qu'a produit un ordinateur qu'à ce qui est manuscrit. Je sais que dans mon cas, bien que je ne devrais pas avoir d'illusions, je ne vérifie pas attentivement les états mensuels de ma carte de crédit, et je pense que c'est dû à la crédibilité qui s'attache à l'imprimé d'ordinateur. Mais nous savons tous qu'une erreur peut se glisser tout aussi facilement dans des états financiers de cette sorte que dans d'autres.

Ce qui me préoccupe, à propos de la recevabilité de ces imprimés d'ordinateur aux fins de la preuve, ce sont les conséquences sur les droits des accusés, en raison même de la

[Text]

printout. It seems to me there is at least as much opportunity for misinformation to creep into a printout as it is into a manual record; perhaps more. There is also the potential for . . . For example, computers are affected by magnetism, and there have been problems with the functioning of computers where steel girders are used in buildings; you find it sets up certain polarity of magnetism which has affected their functioning, which could lead to incorrect information being recorded in a printout, even if the program itself is sound, even if the equipment itself is sound and even if the information inputted was sound.

I do not quite know how to articulate the question, but the concern I have is, particularly in instances where there may not be any trail left that will allow you to reconstruct how the printout came to be, they may have a potentially very dangerous instrument there. It could affect the liberty of individuals and may be unchallengeable by the individual because of the inability to trace back from the document first of all—and, secondly, which has a credibility which is undeserved.

• 1205

Mr. Tollefson: I quite agree with you that the computer is not infallible. I guess the greatest problem with the computer, though, is the operator. If you have people who are punching in the numbers incorrectly or have designed a program that is not as reliable as they think it is—there is some glitch in it somewhere that causes it to spew out false returns from time to time—the old saying about “Garbage in, garbage out” is quite true.

On the other hand, I suppose it is fair to say that many of these same problems, certainly in terms of the human element, apply even more in relation to the old-fashioned handwritten record-keeping systems. One of the arguments that was made to us in the Uniform Law Conference was that there are certainly problems with the computer system and it is true that you can have mechanical or program failures, but when you compare that with the reliability rate of other record-keeping systems you are way ahead with the computer; and there is just no way you can stand in the path of progress . . . the computer will be used whether you like it or not, so get your legislation ready for it.

Mr. Beatty: So essentially your position would be that if you are going to allow other records to be introduced with all the flaws that may be in them you have to be prepared to allow computerized printouts to be introduced.

Mr. Tollefson: I think that is what we have to do, recognizing at the same time that as a matter of weight very frequently you will be able to challenge any record-keeping system by showing that there are possibilities for failure.

Mr. Beatty: I would just close with one observation, and it is one I am sure you will not quarrel with, and that is just to elaborate on the credibility of computers. Fraud artists find computerized statements to be a very useful device, whether it is in phony invoices that are sent out . . . One of the neatest scams—I should not, perhaps, use that terminology, because I

[Translation]

crédibilité du document. Il me semble qu'une information erronée a tout autant de chance de se glisser dans un imprimé d'ordinateur que dans un manuscrit, sinon davantage. Il existe également une possibilité de . . . C'est ainsi que les ordinateurs sont influencés par le magnétisme, et il y a dérèglement du fonctionnement des ordinateurs lorsque des poutres d'acier sont utilisées dans les bâtiments, car elles créent une certaine polarité du magnétisme qui influence le fonctionnement des ordinateurs et pourrait causer des erreurs d'enregistrement d'un imprimé, même si le programme, en soi, est correct, même si le matériel est en bon état, et même si l'information introduite dans l'ordinateur est fiable.

Je ne sais au juste comment présenter la question, mais vous pourriez avoir là un instrument potentiellement très dangereux, en particulier dans les cas où il ne reste aucune trace vous permettant de reconstituer la façon dont l'imprimé a été composé. Cela pourrait porter atteinte à la liberté de l'individu; il se pourrait que l'individu soit incapable de contester, car il ne serait pas possible de remonter à la source du document—du document, d'ailleurs, auquel on a accordé une crédibilité qu'il ne mérite pas.

M. Tollefson: Je suis tout à fait d'accord avec vous lorsque vous dites que l'ordinateur n'est pas infallible. Par contre, le plus grand problème demeure l'opérateur. Si l'opérateur donne des signaux numériques erronés ou s'il a conçu un programme qui n'est pas aussi fiable qu'on peut le croire, on y trouvera un signal transitoire qui fera en sorte que l'ordinateur débitera des imprimés erronés de temps à autre; c'est vrai: la qualité des résultats est fonction de la qualité des données à l'entrée.

Par contre, il est juste de dire que cet élément humain intervient davantage dans l'ancien système de tenue d'archives manuscrites. On a entendu l'argument suivant à la Conférence canadienne de l'uniformisation du droit: malgré la possibilité de pannes, si l'on compare le taux de fiabilité de l'ordinateur à celui d'autres systèmes de tenue d'archives, l'ordinateur est de loin préférable; il est impossible de faire obstacle au progrès—on fera appel à l'ordinateur, qu'on le veuille ou non; il vaut mieux prévoir des mesures législatives.

M. Beatty: Vous dites donc que s'il faut permettre l'entrée d'autres documents, malgré toutes les lacunes qu'ils comportent, il faut être disposé à accepter les imprimés.

M. Tollefson: Il faut le faire, à mon avis, tout en reconnaissant qu'il sera très souvent possible de contester la fiabilité de n'importe quel système de tenue d'archives en exposant les possibilités de pannes.

M. Beatty: J'aimerais terminer en parlant de la crédibilité des ordinateurs, et vous serez d'accord avec moi à ce sujet. Les fraudeurs trouvent les relevés informatisés très utiles, qu'il s'agisse de contrefaçons de factures . . . Une des fraudes les mieux orchestrées—je ne devrais peut-être pas m'exprimer en ces termes, car ce n'est peut-être pas illégal—mais, dans ma

[Texte]

do not think it is against the law—one of the complaints that one often hears in my neck of the woods is about companies that send out invoices for advertising which look very much like they are coming from the phone company. Even if it says in print on the bottom “This is not a bill”, you find that because of the very credibility of the thing, because it looks like a bill, it gets readily paid.

I believe there was also testimony before the McDonald inquiry about the use of social insurance numbers for fraud. The figures I heard were very powerful that because of the very credibility of the social insurance number, the belief that Canadians have that there is only one to a customer, it becomes that much more useful. You have found there were cases where single individuals would have literally dozens and dozens of different unemployment insurance claims under different names using different social insurance numbers. Because of the fact that they had this authentic device, the social insurance number, with its credibility, it enabled them to get in the door in a way they might not have been able to otherwise.

The only concern I have is that an individual might be more susceptible to conviction because of a computerized record and because of an unjustified credibility it might have than he would on the basis of a handwritten record.

I think the point you made was very well taken—that if you are going to allow other records to come in with the flaws they have, you have to do that as well—but it is with some hesitation that I do.

Mr. Tollefson: I suppose, though, that one would have to add that you have the same problem in relation to different kinds of witnesses. If a policeman takes the stand and says something, we have the feeling that quite often the weight of that evidence is greater than if you call an ordinary witness off the street.

Mr. Beatty: That is true.

Mr. Tollefson: Similarly, if you call a witness from the bank who says these are the facts, banking records are very reliable, etc., even if they are the old-style record that is kept with a quill pen . . .

• 1210

Nevertheless, the impact on the court is going to be very great. I do not think there is any system we can devise which will overcome our natural tendency to attribute greater weight to certain kinds of things than others.

Mr. Beatty: Thank you. It has been a very useful education for me.

Thank you, Madam Chairman.

The Chairman: Thank you.

Mr. Robinson.

Mr. Robinson (Etobicoke—Lakeshore): Following up your last statement first, what you are saying in effect is that when

[Traduction]

région, on entend souvent les gens se plaindre du fait que certaines sociétés envoient de la publicité qui ressemble beaucoup à une facture qu'aurait envoyée la société de téléphone. Même si le matériel publicitaire comporte l'avis: «ceci n'est pas une facture», en exergue, bon nombre de gens envoient volontiers l'argent, car le matériel publicitaire a toute l'apparence d'une facture.

Il me semble que la Commission McDonald a également entendu des témoignages au sujet de l'utilisation des numéros d'assurance sociale pour des fins frauduleuses. Cela se fait assez fréquemment, en raison même de la crédibilité du numéro d'assurance sociale, d'autant plus que ce numéro est très utile, étant donné que les Canadiens n'en ont qu'un chacun. Vous avez découvert que certaines personnes avaient fait des dizaines et des dizaines de demandes de prestations d'assurance-chômage sous divers noms, en utilisant différents numéros d'assurance sociale. Vu la crédibilité du numéro d'assurance sociale, ces personnes avaient trouvé une bonne façon de procéder, qui leur permettait de trouver un débouché qu'elles n'auraient pas pu trouver autrement.

Je m'inquiète du fait qu'une personne serait plus susceptible d'être condamnée à cause d'un document informatisé et de la crédibilité injustifiée que celui-ci peut avoir qu'à cause d'un document manuscrit.

Vous avez tout à fait raison. Si l'on accepte les autres documents malgré les défauts inhérents au système, il faut en accepter les conséquences, bien que j'hésite à le faire.

M. Tollefson: Pourtant, le même problème se pose lorsqu'il s'agit de divers genres de témoins. Si un policier vient à la barre, on accordera souvent beaucoup plus de poids à son témoignage qu'à celui d'un citoyen ordinaire.

M. Beatty: C'est exact.

M. Tollefson: Cela vaut également si nous avons affaire au témoignage d'un employé de la banque qui prétend que les dossiers de la banque et les renseignements sont très fiables, même s'il s'agit de renseignements consignés à l'ancienne, avec une plume d'oie . . .

Quoi qu'il en soit, ces témoignages auront beaucoup de poids devant les tribunaux. Je ne crois pas qu'il soit possible de concevoir un système capable de vaincre notre tendance naturelle à accorder beaucoup plus de poids à certaines choses qu'à d'autres.

M. Beatty: Merci. Vos réponses ont été très instructives.

Merci, madame le président.

Le président: Merci.

Monsieur Robinson.

M. Robinson (Etobicoke—Lakeshore): Pour reprendre ce que vous venez tout juste de dire, devant la loi, tous les

[Text]

you are giving evidence, everybody is equal, but some are more equal than others. They are given more credibility, for some particular reason.

Mr. Tollefson: Yes, I agree.

Mr. Robinson (Etobicoke—Lakeshore): I have had cases myself where I have had as many as five witnesses and the judge chose to believe the policeman rather than the five witnesses. Maybe they were not credible witnesses. I thought they were, anyway.

Mr. Beatty: But they were wearing sunglasses at the time.

Mr. Robinson (Etobicoke—Lakeshore): Numbers of witnesses did not make much difference.

Since you have been dealing primarily with the Canada Evidence Act as proposed in Bill S-33, I thought I would ask you two or three questions on that. The first one that comes to mind is this whole question of admissibility. Relating this, of course, to the subject before us, if you can keep that in mind, what is the key to admissibility as you see it when we are talking about computers and crimes related to computers and matters concerning software and all the rest of it? What is the key?

Mr. Tollefson: From a practical point of view, I think the key is evidence of an ongoing system that has been used and experience-rated. In other words, you can call a witness or produce an affidavit to the effect that the system is indeed a very reliable system; it is not something experimental; it is not something that has been used only once. Once you have that in evidence, I think the court says, okay, that is good enough for us.

Mr. Robinson (Etobicoke—Lakeshore): So the primary hurdle, really, is to get admissibility; and once you have overcome that hurdle, everything else is simple. It is just then a question of the weight that is to be given to the accuracy or the authenticity of the evidence, whatever it may be.

Mr. Tollefson: Yes. Whether I would use the word "simple" is another matter. But I do agree with you.

Mr. Robinson (Etobicoke—Lakeshore): But you need to get it admissible.

I notice in this draft legislation that there is no special proposed section on admissibility, except possibly proposed Section 138, which says:

The court shall not exercise evidence or the contents of a record, other than by way of the original or a duplicate, where the unavailability of the original or a duplicate is attributable to the bad faith of the proponent.

Mr. Tollefson: Yes.

Mr. Robinson (Etobicoke—Lakeshore): That is the only thing I can find that refers specifically to admissibility. But this does not refer specifically to the matter with which we are concerned.

[Translation]

citoyens sont égaux, mais certains sont plus égaux que d'autres, dans le cas des témoignages. Pour une raison particulière, on se fie davantage aux témoignages de certains que d'autres.

M. Tollefson: Oui, je suis d'accord.

M. Robinson (Etobicoke—Lakeshore): Dans certaines causes, j'ai moi-même constaté que pas moins de cinq témoins étaient d'accord sur les faits, ce qui n'a pas empêché le juge de croire au témoignage du policier plutôt qu'à celui des cinq autres témoins. Il ne s'agissait peut-être pas de témoins fiables. Mais ils l'étaient, à mon avis.

M. Beatty: Mais ils portaient alors des lunettes de soleil.

M. Robinson (Etobicoke—Lakeshore): Le nombre de témoins ne changeait pas grand-chose.

Mes deux ou trois questions porteront sur la Loi sur la preuve au Canada, aux termes du Bill S-33, puisque vous vous intéressez surtout à ce projet de loi. La première question porte sur la recevabilité. Dans le contexte de nos travaux, quelle est la règle clé de la recevabilité lorsqu'il s'agit d'infractions relatives aux ordinateurs, de logiciels, ou autres? Quel est l'élément clé?

M. Tollefson: Du point de vue pratique, il me semble que cela dépend d'un système qui a été mis à l'épreuve et coté. Autrement dit, un témoin, ou une déclaration faite sous serment, peut indiquer qu'il s'agit d'un système très fiable, qui n'est pas au stade expérimental, qu'il n'a pas été utilisé qu'une fois seulement. Le tribunal acceptera ce genre de preuve.

M. Robinson (Etobicoke—Lakeshore): Le principal obstacle est donc la recevabilité; lorsqu'on a surmonté cet obstacle, le reste est simple. Il s'agit donc du poids à donner à l'exactitude ou à l'authenticité de la preuve, quelle qu'elle soit.

M. Tollefson: Oui. Je ne sais pas si le reste est «simple», cela reste à voir. Mais je suis d'accord avec vous.

M. Robinson (Etobicoke—Lakeshore): Mais la preuve doit être recevable.

Dans le projet de loi, je vois qu'aucune disposition ne vise particulièrement la recevabilité, sauf l'article 138, dont je vous fais la lecture:

La preuve du contenu d'un document par un moyen autre que la production de l'original ou du double est irrecevable si la non-disponibilité de l'original ou du double est attribuable à la mauvaise foi de celui qui entend produire cette preuve.

M. Tollefson: Oui.

M. Robinson (Etobicoke—Lakeshore): C'est la seule disposition que j'ai trouvée qui concerne la recevabilité proprement dite. Mais elle ne s'adresse pas de façon précise à la question qui nous intéresse.

[Texte]

Is the bad faith something that has to be proved or disproved?

Mr. Tollefson: I think the person who asserts that there has been bad faith has the original onus of establishing, at least on a balance of probabilities, that there may be bad faith; there is what you might call an evidential burden upon him to satisfy the court that the proponent of the evidence is not in fact approaching the court with clean hands.

Mr. Robinson (Etobicoke—Lakeshore): In other words, he says, I have destroyed all the records, but from memory I can tell you what was on them. But would not the best-evidentiary rule still apply, in spite of bad faith? Or would you just be thrown out of court?

Mr. Tollefson: If the proponent is established to have been acting in bad faith, then proposed Section 138 says you really go back to the best evidence rule. You have to produce the original, or a duplicate. A "duplicate" means, by proposed Section 130, something that is . . . I will just quote:

• 1215

Duplicate means a reproduction of the original from the same impression as the original, from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent technique that accurately reproduces the original.

Now, in this day and age, I think everybody uses the photocopied copy in much the same way as the original, I suppose. The documents I have before me today are all photocopied. So I think the court really should be able to rely upon that.

Mr. Robinson (Etobicoke—Lakeshore): The document is photocopied, but can you be sure of the accuracy?

Mr. Tollefson: Once again, the bill does suggest in proposed Section 132 that a duplicate is admissible to the same extent as an original, unless the court is satisfied that there is reason to doubt the authenticity of the original or the accuracy of the duplicate.

In other words, if you are wanting to challenge the duplicate, you can either say, look, the duplicate appears to have been altered, it looks like there is some cutting out of something, or a blotting out with a piece of paper or something opaque, in which case the duplicate is no longer an accurate representation of the original, or you can say that the original itself was not authentic; that you started out with something that was not, in fact, the proper document and therefore you cannot make something out of nothing.

Mr. Robinson (Etobicoke—Lakeshore): So the onus then would shift to the person who is objecting to the document.

Mr. Tollefson: Yes.

Mr. Robinson (Etobicoke—Lakeshore): All right. I would like to go back just a step before this into the interpretations

[Traduction]

Faut-il prouver qu'il y a eu ou qu'il n'y a pas eu mauvaise foi?

M. Tollefson: Il me semble que celui qui affirme qu'il y a probablement eu mauvaise foi a le fardeau de le prouver; c'est à lui de prouver au tribunal que la personne qui offre la preuve n'est pas au delà de tout soupçon.

M. Robinson (Etobicoke—Lakeshore): En d'autres termes, elle dit: j'ai détruit tous les dossiers, mais, de mémoire, je peux vous citer les renseignements qu'on y trouvait. Mais, malgré la mauvaise foi, la règle de la meilleure preuve ne vaudrait-elle pas? Le tribunal refuserait-il de vous entendre?

M. Tollefson: S'il est établi que la personne offrant la preuve était de mauvaise foi, l'article 138 du projet de loi prévoit que l'on s'en remettrait à la règle de la meilleure preuve. On est tenu de produire l'original ou le double. Voici ce que l'on entend par le «double»; je lis un extrait de l'article 130:

«Double» provenant de la même matrice ou d'une même impression que l'original, le double produit par photographie, y compris un agrandissement ou une miniaturisation, ou le double produit par enregistrement mécanique ou électronique, par reproduction chimique ou par un autre procédé équivalent propre à assurer une reproduction fidèle de l'original.

Or, de nos jours, il me semble que tout le monde utilise les photocopies comme s'il s'agissait des documents originaux. Tous les documents que j'ai devant moi aujourd'hui ont été photocopiés. Il me semble que le tribunal devrait pouvoir s'en tenir à cela.

M. Robinson (Etobicoke—Lakeshore): Le document a été photocopié, mais pouvez-vous attester de son exactitude?

M. Tollefson: Encore une fois, selon l'article 132 du projet de loi, le double d'un document est recevable en preuve au même titre que l'original, sauf si le tribunal a des motifs de douter de l'authenticité de l'original ou de la fidélité du double.

Autrement dit, si vous voulez contester le double, vous pouvez prétendre qu'il a été altéré, expurgé, de sorte qu'il n'est plus une copie fidèle de l'original, ou vous pouvez prétendre que l'original n'était pas authentique au départ; qu'il ne s'agissait pas du document en question et, par conséquent, que le double ne tient plus.

M. Robinson (Etobicoke—Lakeshore): La charge de la preuve incomberait alors à la personne qui s'oppose à la recevabilité du document?

M. Tollefson: Oui.

M. Robinson (Etobicoke—Lakeshore): Bon. J'aimerais revenir maintenant aux définitions. Vous avez parlé de la

[Text]

clause. You talked about "original" under the definitions part of proposed Section 130, and in (c) it says:

In relation to stored or processed data or information, any printout or intelligible output that reflects accurately the data or information . . .

Are these two terms used interchangeably, or how are they used? They are not, certainly, synonyms.

Mr. Tollefson: No. We did not give a definition of data or information, because . . .

Mr. Robinson (Etobicoke—Lakeshore): You did not have one.

Mr. Tollefson: We felt that there could be evidence as to what is meant by data and what is meant by information. Normally, I do not think it is going to be a major problem. Maybe Mr. Georgas would have a comment on that; but in a particular case I do not think it is going to be a significant problem.

Mr. Robinson (Etobicoke—Lakeshore): Does "information" include data in your view, or are data and information separate?

Mr. Tollefson: I would be inclined to accept his suggestion that data is something that is a bit more organized than information. I do not think we should restrict our consideration of this problem simply to data. It seems to me that there is much information that is contained in computers nowadays that you would not necessarily classify as data but, nevertheless, could be very relevant to a litigation that is going on.

For example, I suppose that nowadays with word processing, and so forth, many letters are stored in the—or in something that would be the equivalent of a computer. You may want to produce a copy from your . . . to show that something happened at a particular time, or that a contract was entered into, or the terms of an offer, and so on. Now, is that data? I would think that is information.

Mr. Robinson (Etobicoke—Lakeshore): I see.

Looking at proposed Section 134, when we talk about other evidence, do you feel that a copy of what was taken would be considered as satisfactory evidence?

Mr. Tollefson: Copy, according to the definitions that appear here, or the system that is set up by the proposed new Canada Evidence Act—that is the lowest possible form of written or hard information.

• 1220

That is to say, you have your original, which is the best; you have your duplicate, which is the second best; but a copy which could be, for example, my just writing down something that I had seen on an original or a duplicate that may not in fact be a complete copy but just notes can nevertheless still be useful to the court. It may be the only thing you have. If you cannot produce either the original or the duplicate, the court is given authority to receive it under proposed Section 134.

[Translation]

définition d'original, à l'article 130; à l'alinéa c), on lit ce qui suit:

Relativement à des données informatisées, tout document intelligible provenant de l'appareil où elles ont été emmagasinées et qui les reflète fidèlement . . .

Peut-on utiliser l'une ou l'autre de ces deux expressions? Ont-elles la même valeur? Il ne s'agit certainement pas de synonymes.

M. Tollefson: Non. Nous n'avons pas défini ces données informatiques, car . . .

M. Robinson (Etobicoke—Lakeshore): Vous n'en aviez pas.

M. Tollefson: Nous avons cru qu'un témoin pourrait faire la distinction entre «donnée» et «information», dans le contexte anglais. En principe, cela ne nous causerait pas de problème majeur. M. Georgas pourrait peut-être vous en dire plus long à ce sujet; mais dans un cas particulier, je ne crois pas que cela soulève un problème d'envergure.

M. Robinson (Etobicoke—Lakeshore): Selon vous, par «information», comprend-on les données, ou s'agit-il de deux réalités bien distinctes?

M. Tollefson: Je suis porté à accepter sa proposition selon laquelle les données sont plus organisées que l'information. Je ne crois pas que notre étude de cette question doive se limiter aux données. Il me semble que de nos jours, bon nombre de renseignements sont emmagasinés dans les ordinateurs, renseignements qui ne seraient pas nécessairement considérés comme étant des données; mais quoi qu'il en soit, ces renseignements pourraient être très pertinents dans le cas d'un litige.

Par exemple, grâce au traitement des textes, bon nombre de lettres sont emmagasinées dans ce que l'on pourrait comparer à des ordinateurs. Il se peut qu'on veuille en obtenir un exemplaire, question de corroborer que telle chose a eu lieu à tel moment ou qu'un contrat a été conclu, ou pour connaître les conditions d'un contrat. Or, peut-on dire qu'il s'agit de données? Ce serait tout simplement des renseignements, de l'information.

M. Robinson (Etobicoke—Lakeshore): Je vois.

L'article 134 porte sur d'autres preuves. Estimez-vous qu'une copie serait considérée comme constituant une autre preuve satisfaisante?

M. Tollefson: Aux termes des définitions, ou du système qui serait créé en vertu de la nouvelle Loi sur la preuve au Canada, on entend, par copie, la forme la plus élémentaire possible de renseignements écrits ou concrets.

Autrement dit, l'original, c'est ce qu'il y a de mieux; le double serait acceptable, faute de mieux; quant à une copie, il s'agirait d'une transcription de ce qu'on lirait sur l'original ou le double d'un document, et il se peut que la copie ne reproduise pas le document dans son intégrité; quoi qu'il en soit, les notes peuvent être utiles au tribunal. Il se peut qu'elles constituent la seule preuve. Si l'on ne peut présenter soit

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): Now I go to proposed Section 153, where we are talking about business records. It states that a business record is admissible even if it is hearsay. I find this incredible. It would seem to me if it said, may be admissible if it is hearsay—but to make the dogmatic statement that it is admissible if it is hearsay I think is a rather dangerous precedent to set.

Mr. Tollefson: Well, I guess it is arguable, at least, that that is the law today under Section 30 of the Canada Evidence Act. The justification for the reception of hearsay in these cases is that the business documents exception to the hearsay rule—and that is what it is, an exception to the hearsay rule—is based upon the assumption that if the document is made in the usual and ordinary course of business, because of the reliance factor that is placed upon those documents and the kind of disciplinary action that can be taken against an individual if he is not careful, if he deliberately puts something down that is not correct, you have a justification for receiving that into evidence.

Mr. Robinson (Etobicoke—Lakeshore): But that is not what this is saying. The proposed section is saying that this exception to the hearsay rule can apply to the admissibility of the document. Then it goes on to say:

... or a statement of opinion ...

But there is a qualification with regard to a statement of opinion, where it says:

... in the case of opinion, to prove that the opinion was given in the usual and ordinary course of business.

But that final statement that it was given in the usual course of business does not apply to hearsay in this section, although you said that it did.

Mr. Tollefson: I said that in terms of the hearsay the justification for allowing, indeed, multiple hearsay into evidence, if it is in a business document, is that if the business is prepared to rely upon multiple hearsay itself, then there is some guarantee of the accuracy or reliability of that information.

It can always be challenged as to its weight. Now think of the business process: you have a record kept by a clerk who receives a particular shipment of things. He enters this information on a slip that is then sent up to the division chief. The division chief sees this record; he adds it to something else and that document is sent on perhaps to a branch manager who looks at it, puts his initials on it, sends it off to the individual who perhaps puts it into a computer. Now if you wanted to avoid the perils of hearsay entirely you would have to call each one of those individuals and ask him: Do you remember this particular document? How was it produced? What steps did you take?

If you recall, the House of Lords when confronted with this problem in relation to the manufacture of cars threw up their hands and said, well, this is a real problem and there is nothing in the law that says we can receive this; therefore they could

[Traduction]

l'original, soit le double, le tribunal peut accepter la copie, aux termes de l'article 134.

M. Robinson (Etobicoke—Lakeshore): Je passe maintenant à l'article 153, où il est question de recevabilité d'un document commercial. Selon cet article, un document commercial est recevable, même s'il s'agit d'un ouï-dire. C'est incroyable. Il me semble qu'on pourrait dire: peut être recevable; mais de là à dire qu'il est recevable, cela constitue un précédent plutôt dangereux.

M. Tollefson: Eh bien, on peut prétendre que c'est la loi, aujourd'hui, aux termes de l'article 30 de la Loi sur la preuve au Canada. La recevabilité des ouï-dire est fondée sur l'hypothèse que si un document commercial est produit dans le cours normal des affaires, étant donné la confiance que l'on manifeste envers ces documents et le genre de mesures disciplinaires pouvant être prises contre une personne imprudente, si cette personne consigne délibérément un renseignement inexact, on pourrait accepter ce document commercial comme preuve. C'est une exception à la règle du ouï-dire.

M. Robinson (Etobicoke—Lakeshore): Mais il ne s'agit pas de cela dans la disposition. L'article prétend que cette exception peut rendre le document recevable. Il peut même s'agir d'un document qui, et je cite:

... exprime un avis ...

Mais on met des réserves à l'avis exprimé ainsi:

... toutefois, ... la preuve doit être faite qu'un avis a été donné dans le cours normal d'une activité.

Mais dans le cadre de cet article, la disposition selon laquelle la preuve doit être faite qu'un avis a été donné dans le cours normal d'une activité ne s'applique pas au ouï-dire, malgré ce que vous avez dit.

M. Tollefson: J'ai dit qu'on justifiait la recevabilité des ouï-dire, et même des ouï-dire multiples, ainsi: dans la mesure où l'entreprise en question est prête à accepter le document commercial sur la foi des ouï-dire, cela constitue, en quelque sorte, une garantie de l'exactitude et de la crédibilité des renseignements.

On peut toujours le contester. Mais parlons d'un cas concret. Un registre est tenu par un commis qui reçoit une livraison de marchandises. Il consigne ces renseignements sur un récépissé qu'il envoie ensuite à son chef de division. Ce dernier en prend connaissance, l'ajoute à quelque chose d'autre, et ce document est envoyé à un directeur de succursale; celui-ci peut le parapher, puis l'envoyer à la personne qui enregistre ces renseignements dans l'ordinateur. Or, si vous vouliez éliminer tous les risques de ouï-dire, il faudrait demander à chacune de ces personnes: vous souvenez-vous de ce document? D'où vient-il? Quelles mesures avez-vous prises?

Vous vous souviendrez que la Chambre des lords a été confrontée à ce genre de problème; il s'agissait de la fabrication de voitures; on a reconnu qu'il s'agissait d'un problème réel et que la loi ne prévoyait pas la recevabilité de ce genre de

[Text]

not accept the records of the company, which indicated that a particular number had been placed on the block of a particular motor. Of course that allowed a group of fraudulent car thieves to get off scot free. I think our position is that we have to accept that, and have to accept business reality; that they cannot indeed call these witnesses, and it would not be possible for these witnesses to remember this information anyway.

• 1225

Mr. Robinson (Etobicoke—Lakeshore): I can appreciate that, but would you not agree with me that the words—and I quote from this proposed Section 153, as follows:

... in the usual and ordinary course of business should apply to hearsay as well as opinion.

Mr. Tollefson: I am sorry. Did you say 153?

Mr. Robinson (Etobicoke—Lakeshore): Yes.

Mr. Tollefson:

A business record is admissible whether or not any statement contained in it is hearsay or a statement of opinion, subject, in the case of an opinion, to proof that the opinion was given in the usual and ordinary course of business.

Our view in the Uniform Law Conference of Canada was that there is a qualitative difference between opinion and what you might call factual information; that an opinion should not be received as part of a business record unless you could establish that opinion as indeed being given as part of the usual and ordinary course of business.

Mr. Robinson (Etobicoke—Lakeshore): On the other point, do you not feel that in the first line of proposed Section 153 the word "is" should be changed to "may be"?

Mr. Tollefson: No.

Mr. Robinson (Etobicoke—Lakeshore): All right.

Mr. Tollefson: I think this would be going back on what the present law is, quite frankly. I think you could, to follow your line of argument, though, sir—you could argue that there might be some limitation on multiple hearsay or something like that, giving the judge the discretion to exclude multiple hearsay if it were shown that there were not other factors which guaranteed the reliability of the information. That is the way I would be inclined to proceed if I were following your approach.

Mr. Robinson (Etobicoke—Lakeshore): So what you are really saying is that where somebody acts upon hearsay of somebody else who, in turn, had acted upon hearsay who, in turn, had acted upon somebody else's hearsay... that sort of thing? So it gets distorted...

Mr. Tollefson: That is right.

Mr. Robinson (Etobicoke—Lakeshore): —but even then, it would still be the best evidence.

Mr. Tollefson: That is right. And the business system may be such that it is really quite accurate information.

[Translation]

preuve; par conséquent, la Chambre n'a pas accepté les documents de la compagnie selon lesquels un certain numéro avait été inscrit sur un certain bloc-moteur. Bien entendu, ce refus a permis à un groupe d'escrocs de s'en sortir indemnes. Nous croyons qu'il faut accepter la réalité du monde des affaires; on ne peut pas faire appel à ces témoins, et ces derniers ne peuvent pas se souvenir de tous les renseignements, de toute façon.

M. Robinson (Etobicoke—Lakeshore): Je comprends cela; mais je vous cite la disposition de l'article 153:

... dans le cours normal d'une activité, il faudrait que cela s'applique également aux ouï-dire ou aux avis.

M. Tollefson: Je vous demande pardon. S'agit-il bien de l'article 153?

M. Robinson (Etobicoke—Lakeshore): Oui.

M. Tollefson:

Un document est recevable en preuve même s'il contient un ouï-dire ou exprime un avis. Toutefois, dans le cas où il exprime un avis, la preuve doit être faite qu'un avis a été donné dans le cours normal d'une activité.

La Conférence canadienne de l'uniformisation du droit a cru qu'il fallait distinguer entre un avis et ce qu'on pourrait appeler un renseignement concret; un avis ne devrait pas être considéré comme un document, à moins que l'on puisse démontrer que l'avis a été donné dans le cours normal d'une activité.

M. Robinson (Etobicoke—Lakeshore): Mais pour revenir à l'autre question, n'êtes-vous pas d'avis qu'il faudrait changer «est» par «peut être», à la première ligne de l'article 153?

M. Tollefson: Non.

M. Robinson (Etobicoke—Lakeshore): Très bien.

M. Tollefson: Il me semble que ce serait régresser par rapport à la loi actuelle, pour vous répondre en toute franchise. Si je poursuis votre argument, on pourrait prétendre qu'il serait bon de limiter le ouï-dire lorsqu'il s'agit d'un certain nombre de personnes, par exemple, ce qui permettrait au juge d'exercer le pouvoir discrétionnaire de ne pas recevoir le ouï-dire en l'absence d'autres éléments corroborant les renseignements. J'aurais tendance à le faire, si j'adoptais votre façon de penser.

M. Robinson (Etobicoke—Lakeshore): Alors, vous dites donc qu'une personne a agi en fonction du ouï-dire d'une autre personne, qui a fait de même, et ainsi de suite. Les renseignements finissent par être faussés...

M. Tollefson: C'est exact.

M. Robinson (Etobicoke—Lakeshore): ... mais malgré cela, ce serait la meilleure preuve possible.

M. Tollefson: Oui. Et il se peut que le système des affaires soit tel qu'il s'agisse de renseignements très justes.

[Texte]

Mr. Robinson (Etobicoke—Lakeshore): The last item I want to ask you about has to do with proposed Section 155. I think you pretty well covered in this proposed section all you would need with regard to computers because you say that the evidence could be adduced by way of affidavit.

Mr. Tollefson: Yes.

Mr. Robinson (Etobicoke—Lakeshore): Do you think this is really sufficient? Affidavit evidence? Somebody swears to something or other, and that is it?

Mr. Tollefson: There is still provision for a person to be called in 156, actually.

... any person who has or may reasonably be expected to have knowledge of the making or contents of any business record or duplicate or copy of it produced or received in evidence may, with the leave of the court, be examined or cross-examined by any party.

In other words, the affidavit is not the end of the line, if there is any doubt about it. The court may say, Yes, in this particular case; we think we ought to have more information and, therefore, the computer operator or the programmer or whoever it may be ought to be called.

Mr. Robinson (Etobicoke—Lakeshore): Thank you very much.

The Chairman: Thank you for appearing before us this morning. I think we have clarified both the Senate bill—and trying to go in the right direction as far as our mandate as concerned.

Before we conclude, I would just remind Mr. Hill that we were expecting some documents from his department. At the beginning of next week before we prepare our report, if they are available, we will be holding some in camera meetings and we would appreciate having them, or it, just as a consultative reference.

I would give it back to you. It would be appreciated. Anyway, Mrs. Hébert will be waiting for the answer from your deputy minister.

Mr. Hill: I can do that now, Madam Chairman. I came prepared to indicate to you and to members of the committee that the document will be made available with no conditions. We unfortunately do not have it in our hands yet. It is somewhere in transit on Air Canada.

The Chairman: All right.

• 1230

Mr. Hill: It is only in one language, unfortunately. That is why we have to give it to you informally.

The Chairman: Okay, it can be made available. Ms Hébert is drafting the report, and I am quite sure she would appreciate having this as part of the documentation available in the preparation of the report. We would be able to consult the document next week; and we will forgive the unilingualism.

[Traduction]

M. Robinson (Etobicoke—Lakeshore): La dernière question que je tiens à vous poser porte sur l'article 155. Il me semble que vous avez bien expliqué comment cette disposition viserait les ordinateurs, car vous avez dit que la preuve serait obtenue par le biais d'une déclaration sous serment.

M. Tollefson: Oui.

M. Robinson (Etobicoke—Lakeshore): Est-ce réellement suffisant, à votre avis? Une preuve obtenue par le biais d'une déclaration faite sous serment? On demande à quelqu'un de prêter serment, et c'est tout?

M. Tollefson: L'article 156 prévoit qu'une personne peut être interrogée ou contre-interrogée.

... une partie peut, avec l'autorisation du tribunal, interroger ou contre-interroger toute personne qui a eu connaissance ou qui est susceptible d'avoir eu connaissance de l'élaboration ou du contenu de l'original, d'un double ou d'une copie d'un document professionnel produit en preuve.

Autrement dit, s'il existe des doutes, on va plus loin que la déclaration sous serment. Dans certains cas, le tribunal peut décider que d'autres renseignements sont nécessaires; dans ce cas, on peut faire appel à l'opérateur ou au programmeur.

M. Robinson (Etobicoke—Lakeshore): Merci beaucoup.

Le président: Je dois vous remercier d'avoir accepté de comparaître devant nous ce matin. Nous avons jeté beaucoup de lumière sur le projet de loi du Sénat, et nous avons fait des progrès par rapport à notre mandat.

Avant de terminer, je tiens à rappeler à M. Hill que son ministère était censé nous envoyer des documents. Au début de la semaine prochaine, avant de commencer la rédaction de notre rapport, nous tiendrons des réunions à huis clos, et nous aimerions pouvoir consulter ces documents, s'ils sont disponibles.

Ces documents vous seraient remis. Nous vous saurions gré de donner suite à notre demande. De toute façon, M^{me} Hébert attendra la réponse du sous-ministre.

M. Hill: Madame le président, je peux m'en occuper tout de suite. J'étais disposé à vous dire, à vous et aux membres du Comité, que le document vous sera remis sans qu'aucune condition vous soit imposée. Malheureusement, nous n'avons pas encore pu mettre la main sur ce document; il se trouve entre les mains d'Air Canada.

Le président: Très bien.

M. Hill: Nous ne l'avons que dans une seule langue, malheureusement. Nous ne pouvons donc vous le donner qu'à titre officieux.

Le président: Très bien, donnez-nous cela tel quel. Je suis sûr que M^{lle} Hébert appréciera de pouvoir s'en servir dans la préparation du rapport. Nous pourrions donc consulter ces documents la semaine prochaine, et nous vous pardonnerons la rédaction unilingue.

[Text]

Mr. Hill: Thank you very much.

The Chairman: Thank you for your help and support. Your department's co-operation was very much appreciated by our committee, and we just hope that our report will help in giving the proper input to your minister so that he can come up with some legislation within a short period of time.

My office will contact your office to decide the timeframe of the drafting committee meeting of next week.

Mr. Robinson (Etobicoke—Lakeshore): Exactly.

The Chairman: I thank everybody for their help and support.

The meeting is adjourned.

[Translation]

M. Hill: Merci beaucoup.

Le président: Je vous remercie pour votre assistance et votre soutien. La collaboration de votre ministère a été très appréciée par notre Comité, et nous espérons de notre côté que le rapport donnera au ministre l'information dont il a besoin pour proposer d'ici peu une loi.

Mon bureau se mettra en rapport avec le vôtre pour fixer des délais au comité de rédaction qui va se réunir la semaine prochaine.

M. Robinson (Etobicoke—Lakeshore): Très bien.

Le président: Je remercie tous les intervenants et les personnes présentes, pour leur assistance et leur soutien.

La séance est levée.



If undelivered, return COVER ONLY to:
Canadian Government Publishing Centre,
Supply and Services Canada,
Ottawa, Canada, K1A 0S9

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
Centre d'édition du gouvernement du Canada,
Approvisionnement et Services Canada,
Ottawa, Canada, K1A 0S9

WITNESSES—TÉMOINS

Mr. Stephen Georgas, Solicitor, Toronto.

Me Stephen Georgas, Avocat, Toronto.

From the Department of Justice:

Mr. E.A. Tollefson, Coordinator, Criminal Code Review;

Du Ministère de la Justice:

M. E.A. Tollefson, Coordonnateur, Révision du Code criminel;

Mr. Norman Hill, Project Chief, Theft and Fraud Project.

M. Norman Hill, Chef de projet, Projet vol et fraude.



HOUSE OF COMMONS
CANADA

REPORT OF THE SUB-COMMITTEE ON COMPUTER CRIME

STANDING COMMITTEE
ON
JUSTICE AND LEGAL AFFAIRS

June 1983

SUB-COMMITTEE

ON COMPUTER CRIME

CHAIRPERSON: Mme Céline Hervieux-Payette, Lib., (Montréal-Mercier, Qué.)
Mr. Ken Robinson, Lib., (Etobicoke-Lakeshore, Ont.)
Hon. Perrin Beatty, P.C., (Wellington-Dufferin-Simcoe, Ont.)

STAFF

Mrs. Monique Hébert, Research Branch, Library of Parliament

Pierre de Champlain

Clerk of the Sub-Committee

HOUSE OF COMMONS

Issue No. 18

Tuesday, June 14, 1983
Thursday, June 16, 1983
Tuesday, June 21, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule n° 18

Le mardi 14 juin 1983
Le jeudi 16 juin 1983
Le mardi 21 juin 1983

Président: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

of the Standing Committee on Justice and Legal Affairs

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

RESPECTING:

Order of Reference

CONCERNANT:

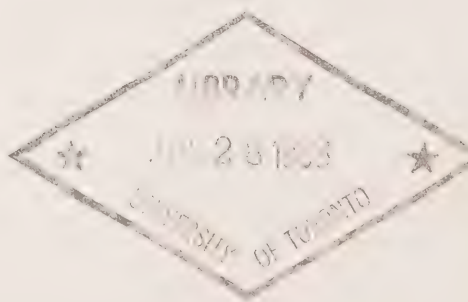
Ordre de renvoi

INCLUDING:

Final Report

Y COMPRIS:

Rapport final



First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

Published under authority of the Speaker of the House of Commons by the
Queen's Printer for Canada

Available from the Canadian Government Publishing Center, Supply and
Services Canada, Ottawa, Canada K1A 0S9

Publié en conformité de l'autorité du Président de la Chambre des communes
par l'Imprimeur de la Reine pour le Canada

En vente: Centre d'édition du gouvernement du Canada, Approvisionnement et
Services Canada, Ottawa, Canada K1A 0S9

NINTH REPORT

In accordance with its Order of Reference of Wednesday, February 9, 1983, your Committee assigned responsibility for the study of the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, to a Sub-committee.

The Sub-committee has submitted its final report to the Committee. Your Committee has adopted this report with amendments and asks that the Government consider the advisability of implementing the recommendations contained in the report.

The report of the Sub-committee, as amended, reads as follows:

TABLE OF CONTENTS

	Page
RECOMMENDATIONS	7
INTRODUCTION	9
A. The Computer Phenomenon	11
B. The Incidence of Computer Crime	13
C. The Criminal Law: The Existing Framework	14
D. The Criminal Law: Proposed Amendments	15
E. The Canada Evidence Act	17
F. The Problems of Law Enforcement	18
G. Additional Measures	18
1. Security Standards.....	18
2. Civil Remedies	19
3. Code of Ethics/Code of Conduct	20
CONCLUSION	22
REQUEST PURSUANT TO STANDING ORDER 69(13) OF THE HOUSE OF COMMONS.....	22
NOTES	23
APPENDIX "A": LIST OF WITNESSES.....	25
APPENDIX "B": SELECTED BIBLIOGRAPHY	27

RECOMMENDATIONS

1. The Sub-committee recommends that the *Criminal Code* be amended to create two new offences: the unauthorized access (without colour of right) to a computer system, and the unauthorized alteration or destruction (without colour of right) of computerized data. The Sub-committee further recommends that Crown prosecutors be given the option of proceeding either by indictment or by way of summary conviction (para. 37).

2. The Sub-committee recommends that the definitions necessary to the description of the substantive offences be expressed, to the greatest extent possible in terms of function rather than of technology (para. 38).

3. The Sub-committee recommends that a comprehensive review of all matters relating to the effective detection and prosecution of computer crime be undertaken. Special attention should be paid to the adequacy of existing powers of search and seizure, the federal acts and treaties relating to international investigations and extraditions, and the wire-tap provisions of the *Criminal Code* as they relate to communications between computers (para. 47).

4. The Sub-committee recommends that every effort be made to ensure that law enforcement agents and prosecutors who are likely to deal with cases involving computer crime receive the necessary computer training to carry out effectively their functions (para. 48).

5. The Sub-committee recommends that the computer industry and institutional users recognize the potential for computer crime and adopt appropriate security measures (para. 51).

6. The Sub-committee recommends that the *Copyright Act* be amended to include computer software (para. 55).

7. The Sub-committee recommends that the federal government undertake a comprehensive study to examine the feasibility of extending patent and industrial design protection to computer programs (para. 56).

8. The Sub-committee recommends that both levels of government undertake a comprehensive joint study of trade secrecy law and adopt corrective measures (para. 58).

9. The Sub-committee recommends that the computer industry ensure, through self-regulation, a high standard of conduct in the industry (para. 65).

10. The Sub-committee recommends that knowledge of computer ethics be a qualification for educators involved in teaching computer skills and that the ethics of computer use be integrated into computer classes at all levels. (para. 67).

INTRODUCTION

1. The mandate of your Sub-committee is to examine the subject-matter of Bill C-667, an Act to amend the *Criminal Code* and the *Canada Evidence Act* in respect of computer crime.

2. Introduced for first reading by the Honourable Perrin Beatty on December 16, 1982, Bill C-667 was withdrawn from second reading on February 9, 1983, and its subject-matter referred to the Standing Committee on Justice and Legal Affairs. A Sub-committee representing the three parties was established on March 10, 1983. The actual working group consisted of the Chairperson, Maître Céline Hervieux-Payette, Mr. Kenneth Robinson, Q.C., M.P., and the Honourable Perrin Beatty, M.P.

3. This arrangement, in the Sub-committee's view, worked out extremely well. Our limited membership and capacity to establish a non-partisan atmosphere in the course of our deliberations combined to make our work both effective and productive. For these reasons, we suggest that small sub-committees should be utilized more frequently to deal with the many issues which are of concern to Parliament.

4. In the course of our hearings, which began on March 17, 1983, the Sub-committee heard considerable evidence from a wide range of witnesses.(1) Appearing before us were individuals and groups with expertise in such diverse fields as computer technology, security and management, computer law, the law of intellectual property, law enforcement, banking, privacy rights and consumer protection.

5. The Sub-committee is deeply indebted to these persons who so generously gave of their time and expertise. The many different views expressed were extremely useful in providing us with a proper perspective on many of the issues at hand. We are especially grateful to the officials from the Department of Justice whose co-operation and assistance were unfailing, and to Ms. Susan Hubbell Nycum of the California law firm of Gaston, Snow and

Ely Bartlett, who was kind enough to share with us her knowledge of the American experience. The Sub-committee also wishes to acknowledge its gratitude for the assistance given in the course of the study and preparation of its report by the Clerk of the Sub-committee, Mr. Pierre de Champlain, and Mrs. Monique Hébert of the Research Branch of the Library of Parliament.

Céline Hervieux-Payette
Chairperson

A. The Computer Phenomenon

6. Since it was first introduced in 1946,(2) the computer has come to play such a dominant role in the processing of all kinds of information that it is difficult to imagine any large-scale enterprise able to function without it. According to industry sources, close to \$40 million are transferred every day by electronic computer systems in Canada. In the United States, this figure is closer to \$400 million. World-wide, it is \$600 million.(3)

7. An indispensable tool to both business and government, the computer is now making inroads into the personal home market with typewriter size consoles that use the television screen for their video display. Anyone who has a bank account or engages in any kind of credit transaction routinely comes into contact with computers. As one witness appearing before the Sub-committee aptly put it:

“Today I have come into contact with at least three computers since I left home in Toronto this morning. I flew to Montreal first thing this morning and Air Canada’s computer gave me a boarding pass. I came on Via rail at lunchtime, and that gave me a ticket. Then I went to the Bank of Commerce, used my VISA card and drew out \$100.”(4)

The computer, in brief, is being integrated into every facet of human activity. It has the ability to collect, store, correlate, transfer and retrieve large amounts of data with relative ease and speed. While its present usefulness is undeniable, future technological advances will make it virtually indispensable.

8. However, there is an ominous side to be considered. Because of the computer’s ability to process quantities of valuable information, it has become an obvious and attractive target of abuse. One hears of “system hackers” who, with some elementary knowledge of how computers function, gain access to telephone terminals and personal microcomputers. Contests are held in universities to see which student will be the first to break the computer’s security—sometimes with the instructor’s encouragement. Sophisticated fraud artists may steal thousands, and perhaps millions, of dollars from financial institutions by using the computer to reroute penny fractions into fictitious accounts. Disgruntled employees may place “time-bombs”* in the computer system, which are set to go off and destroy valuable programming once the employee has left the company.

9. Two well publicized “system hacking” incidents occurred in Canada. First, in the Dalton School case of 1980, a group of Grade Eight students from a private school in New York used the school’s microcomputer to gain access to the data bases of a number of

* A “time-bomb” or “logic bomb” is a computer program inserted into a computer system, which damages the computer software or hardware, under predetermined circumstances. For example, a payroll system programmer could put a logic bomb in the computerized personnel system so that, if his name is ever removed from the personnel file, indicating termination of employment, a secretly coded program would be triggered resulting in the entire personnel files being erased.

Canadian companies and the federal government. Their method was not complicated. On the basis of published computer telephone numbers, the students were able to connect into the Canadian computers and, by simply trying out different passwords until one worked, succeeded in gaining access. Attempts were made on 21 Canadian computer systems. However, these attempts were not all successful. Some systems were well protected with sophisticated controls and codes. Only two firms indicated that their data banks had actually been penetrated and some information destroyed.

10. The second case occurred at the University of Alberta. In the summer of 1977, the University's computer was experiencing an unusually high degree of shutdowns, otherwise known as computer "crashes". Suspecting foul play, the University personnel, after close monitoring, apprehended a high school student who was in the process of using the computer system from one of the remote terminals located on campus. The student was not authorized to use the computer. He was charged with the offences of mischief, contrary to section 287(1)(c) of the *Criminal Code*(5) and the illegal use of a telecommunication facility, contrary to section 287(1)(b). Two other suspects also were charged with aiding and abetting in the commission of the offences, contrary to section 21(1) of the *Criminal Code*.

11. At trial, one accused was acquitted because of the lack of evidence. The second, the high school student caught red-handed, was found guilty on both counts. The third, the accused McLaughlin, was found guilty on the second count, but was acquitted on the mischief charge, since the evidence failed to establish his actual involvement in the computer "crashes".(6) McLaughlin appealed his sole conviction. On the ground that a computer system did not constitute a "telecommunication facility", the Alberta Court of Appeal, in a two-to-one decision, allowed the appeal and set aside the conviction, a ruling which was sustained in the Supreme Court of Canada.(7)

12. The *McLaughlin* case is important because it demonstrates that, for certain kinds of conduct which otherwise would be viewed as criminal, no criminal offence is committed since the provisions of the *Criminal Code* simply are inadequate. Since the relevant provisions of the *Criminal Code* were drafted at a time when computers did not exist, their formulation is not completely attuned to the new technology. Yet, with a rapidly advancing technology, the computer can be expected to play an ever-increasing role in our daily affairs. The need for legislative action to keep pace with this emergent technology and protect society from its ill-effects is apparent. Given the computer's capacity to process large amounts of valuable information, whether of a commercial or personal value, appropriate measures must be taken now before substantial economic or personal loss is sustained.

13. Witnesses appearing before the Sub-committee agreed that criminal sanctions were required to fill the void left by the *McLaughlin* case. However, there was little agreement on the form they should take. A number of witnesses argued that criminal sanctions should constitute but one of a variety of possible solutions, that emphasis should also be placed on improving the existing remedies or creating new ones. This view is shared by the members of the Sub-committee. In our opinion, it is important that all possible avenues of redress be examined and made available, where appropriate, so that the criminal law will be used only when necessary.

14. It may be useful at this juncture to mention that the term "computer crime", while a useful form of shorthand, is a misnomer. The more appropriate reference would be "com-

puter-related" or "computer-associated" activities. Moreover, since anti-social acts considered to be criminal in nature do not constitute a "crime" in Canada unless they are prohibited by law, it follows that the correct term which should be utilized is "computer-related" or "computer-associated misconduct". Indeed, the mandate of the Sub-committee is to propose amendments to the *Criminal Code* which would make a "crime" of those acts of "computer-related misconduct" not currently prohibited. Having raised this technical point, the remainder of this Report will refer to the term "computer crime" for the sake of convenience, whether the misconduct actually constitutes a crime or not.

B. The Incidence of Computer Crime

15. By all accounts, the incidence of computer crime is difficult to estimate. Some over-estimation may occur because any offence remotely associated with a computer is described as a computer crime. For instance, if a dishonest bank employee manually falsifies financial records which are subsequently fed unaltered into the bank's computer, no longer is this form of embezzlement called a fraud. Instead, a computer crime is committed, irrespective of the actual role played by the computer in the commission of the offence. Similarly, where a person is able to withdraw funds fraudulently from an automated banking device because he stole a credit card and obtained the password, again it is described as a computer crime, rather than the plain theft of a credit card. There is, in other words, a tendency to sensationalize what are otherwise fairly common offences.

16. Another reason why the incidence of computer crime is largely unknown is that the crimes may go undetected by the victim or, if detected, may go unreported, since victims, particularly those in the business community, may prefer not to attract any adverse publicity. Other reasons may be that the matter can be adequately dealt with internally, or the loss is too insignificant to warrant serious action.

17. There is very little empirical data which clearly demonstrate that computer crime poses a serious problem. According to a survey conducted by the Ontario Provincial Police between 1980 and 1981, of the 321 responses received from the 648 companies canvassed, only 13 reported experiencing a loss through computer crime, two-thirds of which involved theft of computer processing time and malicious damage to the computer files or equipment. Of these 13 incidents, only five were reported to the police at the time, and only three prosecutions appear to have been undertaken.(8)

18. Representatives from the Canadian Bankers' Association testified that, to their knowledge, members of the Association had never experienced a "pure" computer crime, one where the computer was instrumental in, rather than incidental to, the commission of an offence. Other evidence suggests that approximately 75 cases are reported annually worldwide, with a total annual loss of approximately \$40 million.(9)

19. This evidence is in stark contrast to the often-heard "tip of the iceberg" theory which suggests that 85% of all computer crimes go unreported, with estimated annual losses in the billions of dollars. The evidence presented to the Sub-committee does not support this high estimate. Based on the testimony given, it is probably safer to conclude that the actual incidence of computer crime simply is not known. A comprehensive study has never been undertaken in Canada to estimate the occurrence rate and we do not feel that one is neces-

sary at this time. In our opinion, the fact that relatively little is known about the incidence and seriousness of computer crime is not a justification for legislative complacency. We must still have regard for the potential harm to society. Legislative action is needed to proscribe actual crimes and deter offenders.

C. The Criminal Law: The Existing Framework

20. One conceptual way of approaching computer crime is to distinguish between the computer as an instrument of crime, and the computer as the object of crime.

21. In the first category, the computer is used as a tool in the commission of the offence. The offence itself is not new. Only the means by which it is carried are new. The most important class of offences falling within this category are the computer-assisted frauds, that is, offences which have been successfully prosecuted under the existing provisions of the *Criminal Code*.

22. The second category, where the computer is the object of crime, is not so clear-cut. There are the "physical" offences, where there is tangible damage to, or the physical theft of, the computer or its components. Included in this category are the conventional theft and mischief offences. These offences also are successfully prosecuted under existing law.

23. The real problem arises when the computer, as the object of crime, sustains no tangible damage, as was the situation in the *McLaughlin* case. It will be remembered that McLaughlin was acquitted on the mischief charge because there was insufficient evidence linking him to the computer "crashes". Unless there is some kind of actual interference with the lawful use, enjoyment or operation of the computer, the mischief provisions of the *Criminal Code* will likely be inadequate.

24. An attempt recently was made to bring the activity within the general theft provisions of the *Criminal Code*. In the case of *R. v. Stewart*(10), the Crown alleged that the accused Stewart was guilty of counselling the theft of "information" belonging to the complainant hotel when the accused approached a hotel employee in order to obtain a copy of the computerized list of employees which contained their names, addresses and telephone numbers. This computer list, apparently, was to be used for the purpose of unionizing the hotel employees.

25. The trial judge dismissed the Crown's submissions, holding that the term "anything" whether tangible or intangible, used in the theft provisions of section 283 of the *Criminal Code* had to be capable of being property. Confidential information such as a list of employees was not property for the purpose of the law of theft. Anyone who takes or converts confidential information only, it was held, does not take or convert "anything" as that term is contemplated by section 283.

26. Since the Supreme Court of Canada effectively ruled out the possibility of equating computers with a telecommunication facility, a variety of activities violating the integrity of the computer system is not proscribed.

27. The nature of the activity involved in these abuses which are not prohibited under the *Criminal Code* covers a broad range. At one end of the spectrum is the so-called "joy-

riding” where essentially harmless “trespassers” seek the adventure and challenge of breaking into someone else’s data base, without any intention of altering or destroying the data. At the other end of the spectrum is the more serious and sophisticated industrial espionage, where a competitor copies, without leaving any traces, computerized information which is both confidential and valuable, such as information on a large land development project or new oil discoveries. Even if the information has no economic value, the potential for injury may be great. For instance, a wrongdoer could gain access to computerized personnel files and use the information for a variety of improper actions.

28. Regardless of the severity of the abuse, the Sub-committee is of the view that criminal sanctions are necessary to curb this kind of conduct. This view was widely shared by all witnesses appearing before us. However, there was no clear consensus as to the exact nature such reform should take.

D. The Criminal Law: Proposed Amendments

29. Some witnesses argued that the definition of the term “property” should be extended to cover “information” or “computer-stored information” so that the existing provisions of the *Criminal Code* could apply. The Sub-committee questions this approach. In our view, it would be ill-advised to grant a proprietary interest in information per se, something which does not exist even in the civil law. For reasons of public policy, the exclusive ownership of information, which, of necessity, would flow from the concept of “property”, is not favoured in our socio-legal system. Information is regarded as too valuable a public commodity to have its ownership vest exclusively in any particular individual.

30. Even with the statutory monopolies of copyright, patent, trademark and industrial designs, the creator, inventor or designer of the work is not given exclusive ownership rights in his creation, invention, or design. What is granted is more akin to an exploitation right, for a limited period of time. For example, the author of a book has, under the *Copyright Act*,⁽¹¹⁾ the sole right to “produce or reproduce” his book. Others are not precluded from drawing from the book. They simply may not make copies of it or copy its content, as that is the exclusive right of the author and his assignees, for the author’s life plus 50 years. Similar, though not parallel, considerations come to bear with the remaining statutory monopolies. For these reasons, we believe that extending the definition of “property” to include “information” may lead to more problems than it would resolve.

31. A second reason to avoid this course of action is that it would confer on computer-stored information a status different to that of conventionally stored information. We are not persuaded that the medium of storage should govern the legal protection extended. Information taken from a filing cabinet or a computer is nevertheless stolen information. In our view, in order to be consistent, information must be given an even treatment, regardless of its storage medium.

32. Another possibility is the creation of an entirely separate statute specifically to deal with all matters relating to the computer. This possibility, which was not recommended by any witness appearing before us, is problematic for several reasons. Firstly, in order to introduce worthwhile legislation, far more time and study would be required in order to obtain a proper perspective. In our view, it is more important to introduce limited amend-

ments than to await the introduction of an all encompassing statute. Secondly, for the reasons stated above, it would be undesirable to treat computer crime differently than any other crime. If the conduct is criminal in nature, it properly belongs in the *Criminal Code*. Thirdly, it is unlikely that Parliament has the necessary legislative jurisdiction to enact such a law, given the potential for conflict with the provinces' legislative authority.

33. The prevalent view expressed by the witnesses appearing before us involves the creation of distinct provisions in the *Criminal Code* specifically to protect the integrity of computers. One of these would make the unauthorized access to a computer system a crime. In a draft proposal submitted to the Sub-committee, the Canadian Bar Association proposes that "everyone who, without lawful excuse, obtains the use of a computer system or any part thereof, without the consent of the owner" be made a criminal offence. Variants of this proposal which have been suggested, although not in legislative form, consist of making it an offence to interfere without lawful authorization with a computer, to use the computer in an unlawful manner, to take data without authority or to obtain computer services without authorization.

34. A number of witnesses recommended that a second offence should be enacted to proscribe the more reprehensible conduct of actually doing something to the data once access to the computer has been gained. In this regard, the Canadian Bar Association recommends the creation of an additional measure whereby an offence would be committed by "everyone who, without lawful excuse, alters or destroys computer programs or computer software without the consent of the owner." This approach, which deals with the alteration or destruction of data, is fairly representative of those who favour an additional offence.

35. The Sub-committee is in general agreement with this approach. However, an argument can be made that the second offence is already covered by the simpler "unauthorized access" offence, and that the seriousness of the abuse can adequately be addressed by making the offence a "dual procedure" offence and by providing for a broad range of sentences.

36. The Sub-committee does not support the latter view. In our opinion, the expediency factor must give way to the requirement that the criminal law be precise and fair. There is, in our view, a substantial difference between the two types of misconduct. They should not be dealt with on the strength of the same evidence.

37. The Sub-committee therefore recommends that the *Criminal Code* be amended to create two new offences: the unauthorized access (without colour of right) to a computer system, and the unauthorized alteration or destruction (without colour right) of computerized data. The Sub-committee further recommends that Crown prosecutors be given the option of proceeding either by indictment or by way of summary conviction.

38. The Sub-committee does not favour any specific wording of the proposed amendments. However, we have been repeatedly forewarned of the dangers of tying the definitions down to the current technology. Great improvements are being made in the area of computer technology. It is crucial that the definitions utilized avoid technical terms likely to be obsolete in the foreseeable future. It is therefore recommended that the definitions necessary to the description of the substantive offences be expressed, to the greatest extent possible, in terms of function rather than of technology.

39. As discussed earlier, the incidence of computer crime is largely unknown. In order to assess properly the dimensions of the problem, some contend that it would be desirable to enact compulsory reporting provisions. The Sub-committee does not favour this approach. Compulsory reporting provisions are not generally required under the *Criminal Code*, even with the most serious crimes such as homicide. To require that computer crimes be reported when most other offences are not cannot be justified, in our view. Moreover, to enact such a provision would be ill- advised, given its largely unenforceable nature.

E. The Canada Evidence Act

40. Part of the Sub-committee's mandate was to examine possible amendments to the Canada Evidence Act. Section 6 of Bill C-667 proposed to amend the existing *Canada Evidence Act* by providing that computer printouts be treated as original documents for the purpose of their admissibility into evidence.

41. This above amendment appears to have been proposed in response to the 1979 case of *R. v. McMullen*.⁽¹²⁾ In this case, the court held that, in order to admit computer printouts into evidence, the nature and kind of evidence required would have to reflect the facts of the complete record-keeping process which, in the case of computer printouts, included the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation. If such evidence was beyond the ken of the manager, accountant or the officer responsible for the records, it was stated that the printout would not be admissible.

42. This ruling was not well received, particularly by the representatives of financial institutions. They objected both because it contemplated the introduction of evidence which might expose their computer security—since the computer processes and procedures had to be proven—and because it might require the testimony of too many bank employees who would need time off from work in order to give their evidence in court.

43. The *McMullen* case appears to have been largely superseded by the more recent case of *R. v. Bell and Bruce*.⁽¹³⁾ The latter case decided that computer printouts constituted "records" within the meaning of section 29(2) of the *Canada Evidence Act*, since they were the only source of reference available to the bank as to the state of its bank accounts. As a "record" coming within the meaning of s. 29(2), the computer printout would be admissible on the strength of affidavit evidence.

44. Since the decision in *Bell and Bruce*, the alleged difficulties raised in the *McMullen* case appear to have resolved themselves in practice, although there is still much debate in academic circles as to the actual extent to which *Bell and Bruce* overrules the *McMullen* case.

45. The Sub-committee has received little evidence on this aspect of its mandate. On November 18, 1982, the government introduced Bill S-33, an Act to give effect, for Canada, to the Uniform Evidence Act adopted by the Uniform Law Conference of Canada. Bill S-33, which *inter alia* deals with the admissibility of computer printouts, is before the Senate Standing Committee on Legal and Constitutional Affairs. It is therefore not our intention to

make specific recommendations: the Sub-committee is satisfied that the provisions of the Bill are receiving every consideration. However, we affirm the importance of the work before the Senate Committee.

F. The Problems of Law Enforcement

46. By their nature, computer crimes are not easily detectable. Evidence presented to the Sub-committee suggests that, with some computer crimes, discovery is frequently no more than a matter of chance. The Sub-committee appreciates the complexities associated in effectively detecting and successfully prosecuting computer crimes, particularly those involving transborder data flows. Because of this fact, there is a real need further to develop the procedures available to detect and to gather the necessary evidence.

③ 47. The Sub-committee therefore recommends that a comprehensive review of all matters relating to the effective detection and prosecution of computer crime be undertaken. Special attention should be paid to the adequacy of existing powers of search and seizure, the federal acts and treaties relating to international investigations and extraditions, and the wire-tap provisions of the *Criminal Code* as they relate to communications between computers.

④ 48. To state that the techniques and powers of law enforcement must be adequate to deal effectively with computer abuses is addressing but one dimension of the problem. Another dimension rests with the need to ensure that the personnel assigned to detect and prosecute computer crimes obtain the necessary computer expertise. Computers are complex systems which can easily overwhelm those who have little or no knowledge of the field. The Sub-committee therefore recommends that every effort be made to ensure that law enforcement agents and Crown prosecutors who are likely to deal with cases involving computer crime receive the necessary computer training to carry out their functions effectively.

G. Additional Measures

1. Security Standards

49. As stated earlier, the Sub-committee firmly believes that the criminal law should constitute only one of the possible solutions to computer crime. Of all the other measures which were presented, the most important, in our view, are those which involve security measures.

50. Evidence presented at the hearings suggests that many computer crimes could have been averted if proper security measures had been implemented. The need for self-regulation within the industry is apparent. In our view, all computer systems which store valuable information, whether of commercial or personal value, must at least meet adequate security standards.

⑤ 51. The Sub-committee does not recommend compulsory security standards, although they have been suggested by a few witnesses. It may well be that, at some future date, there

will be a need to enact appropriate regulations. In the interim, we recommend that the computer industry and institutional users recognize the potential for computer crime and adopt appropriate security measures.

2. Civil Remedies

52. Civil remedies are an important complement to the criminal law. In many instances, the victim of a computer crime may not want to press charges against the perpetrator, preferring to bring a civil action in order to get compensation for the loss sustained. For instance, if a video game pirate steals a program and then proceeds to sell pirated copies of the game, the program's creator may prefer to recoup his or her losses rather than send the offender to prison. Knowing that the offender is incarcerated may be of little consolation to a victim who, because of the piracy, is on the verge of bankruptcy.

53. The civil remedies which fall under federal jurisdiction are the statutory monopolies of copyright, patent, industrial design and trademarks. Of these, copyright and patent law appear to offer the best hope of providing some form of relief to the victim where the object of crime is the computer software. However, the weight of opinion seems to favour copyright protection.

54. Under the current *Copyright Act*, computer software is not specifically included in the protected works under the Act. In practice, many creators claim copyright for their programs, but the law itself is uncertain. We have heard evidence from a number of copyright experts who are convinced that copyright protection is the most appropriate vehicle. In 1978, the United States amended its copyright laws to include computer software, following a thorough study by a presidential committee on new technological uses.

55. The Sub-committee notes that a revision to the Canadian *Copyright Act* is in the final stages of preparation. Consistent with our view that the victims of computer crime should have as many avenues of redress as possible, we believe that copyright protection should be extended to computer software products. We therefore recommend that the *Copyright Act* should be amended to include computer software.

56. It may be that patents and industrial designs offer possibilities for the protection of computer programming. Because the Sub-committee received little testimony of this issue, we refrain from making a judgement. We recommend, however, that the federal government undertake a comprehensive study to examine the feasibility of extending patent and industrial designs protection to computer programs.

57. As with the federal statutory monopolies, the law of trade secrecy is underdeveloped. At present, trade secrets protection, which exists only at common law, works fairly well when there is a clear confidential relationship between two parties as, for example, in the case of an employee who is bound to respect the confidential information received in the course of his employment. The protection becomes more doubtful when the trade secret is conveyed to third parties who are not themselves privy to the original agreement of confidentiality.

58. The Sub-committee believes that the law of trade secrecy could be vastly improved to offer more protection to all victims whose trade secrets have been breached, either because of a computer crime or in other ways. Losses resulting from the theft of trade secrets can be

extensive. At present, trade secrecy is a matter falling within provincial jurisdiction and no province has enacted trade secrecy legislation. In the future, a need to criminalize the theft of trade secrets may arise. The Sub-committee, however, recommends that both levels of government undertake a comprehensive joint study of trade secrecy law and adopt corrective measures.

59. Given the computer's incredible capacity to collect and process data, many are deeply concerned about its potential threat to the confidentiality of personal information. Privacy rights advocates even have recommended that the custodians of personal information should be held criminally liable for unlawful access to the information due to inadequate security. While sympathetic to their concerns, the Sub-committee cannot support such drastic measures at this time. However, steps should be taken to ensure that personal information, whether stored in a computer or elsewhere, is adequately protected from those who have no right to have access to it.

60. Privacy rights are largely a matter of provincial jurisdiction, but no province has taken the initiative to enact comprehensive measures to deal with the protection of all personal information. The province of Quebec may be cited for its innovative law on access to public documents and the protection of personal information.(14)

61. The basic framework of the Quebec law is that information publicly held is to be treated confidentially unless the person the information concerns authorizes its disclosure. Moreover, the government can issue regulations fixing the appropriate security standards to ensure the information's confidentiality. Finally, penal sanctions are provided for any unlawful disclosure of publicly held personal information.

62. While there are a number of measures which exist under other federal and provincial statutes which provide for the confidential handling of personal information, for example, sections 62 and 63 of the federal *Privacy Act* and section 241 of the *Income Tax Act*,(15) no truly comprehensive privacy statute has been enacted. This underdeveloped area of the law, in our view, should be subject to further study.

3. Code of Ethics/Code of Conduct

63. Since the computer industry is relatively new, few measures govern the activities of those who work with computers. Although the information contained in the computer may be highly valuable or sensitive, there are no compulsory codes of professional conduct which must be adhered to, as is required for other disciplines, such as law and medicine. The Canadian Association of Data Processing Service Organizations (CADAPSO) has developed a code of conduct which has provisions dealing with standards of conduct affecting the public interest, and relations with members and non-members engaged in the provision of data processing services.(16) However, membership in CADAPSO is not mandatory.

64. The Canadian Information Processing Society (CIPS) is in the process of developing a certification accreditation process for systems programmers so that the industry can regulate itself. At this time, the process is nowhere near completion.(17)

65. The Sub-committee supports these efforts which may deter would-be computer criminals and ensure a high standard of moral behaviour among computer users. If self-regulation fails, compulsory accreditation or licensing may have to be considered, but the current

situation does not justify such action. The Sub-Committee therefore recommends that the computer industry ensure, through self-regulation, a high standard of conduct in the industry.

66. There is growing evidence that users of computer systems are not, in all cases, aware of their ethical responsibilities. Adolescents and young students are of special concern because their level of maturity can be far less developed than their computer skills.

67. The Sub-committee believes that much could be gained if proper ethical conduct were made an integral part of computer training. If appropriate ethical values are instilled in the individual at an early date, they may serve to decrease the potential for computer crime. The Sub-committee therefore recommends that knowledge of computer ethics be a qualification for educators involved in teaching computer skills and that the ethics of computer use be integrated into computer classes at all levels.

68. Early in its deliberations, the Sub-committee became aware that it was impossible to separate the issue of computer crime from the much broader issue of "information". Because of this observation, we have made recommendations in areas which may well go beyond our narrower mandate of computer crime and the criminal law. Nevertheless, we believe that it is desirable to have all possible remedies in place. Amendments to the *Criminal Code* constitute only one of these. In terms of deterrence, the fact that a computer criminal may be liable for damages for the loss occasioned by his or her misdeed can be as effective a deterrent as the imposition of a fine or a term of incarceration.

69. Improved remedies are therefore necessary to provide the victim of a computer crime with the most suitable form of redress. These measures, however, arise only after the crime has been committed. In our view, it is of greater importance to ensure that all possible preventive measures are vigorously pursued. If computer systems are adequately secured, and those most likely to use them are properly educated, a number of wrongful acts which otherwise might occur will be averted.

REQUEST PURSUANT TO STANDING ORDER 69(13) OF THE HOUSE OF COMMONS

70. Pursuant to Standing Order 69(13) of the *Permanent and Provisional Standing Orders of the House of Commons*, the Committee on Justice and Legal Affairs requests that the Government table a comprehensive response within 120 days of the presentation of this Report to the House of Commons.

NOTES

- (1) For the list of witnesses appearing before the Sub-committee, see Appendix "A"
- (2) The first computer came into existence in 1946 at the University of Pennsylvania. It was called the "Electronic Numerical Integrator and Calculator" (ENIAC). For greater detail, see S. Sokolik, "The Computer Crime—The Need for Deterrent Legislation" *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, pp. 353-385, at p. 354.
- (3) *Security World*, January 1982, p. 28.
- (4) Evidence given by Mr. Peter Ward of Peat, Marwick and Partners. *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, April 27, 1983, 4:18.
- (5) R.S.C. 1970, c. C-34.
- (6) *R. v. Christensen et al.* (1978), 26 *Chitty's Law Journal*, p. 348 (Supreme Court of Alberta, Trial Division).
- (7) *McLaughlin v. R.* (1979), 12 C.R. (3d) 391 (Alberta Court of Appeal); and *Her Majesty the Queen v. McLaughlin* (1980) 2 S.C.R. 331 (Supreme Court of Canada).
- (8) Entitled the "Ontario Provincial Police, Computer Crime and Security Survey", this survey was produced by Superintendent G.W. Allen, of the Commercial Crimes Branch of the R.C.M.P., who appeared before the Sub-committee on March 17, 1983.
- (9) Evidence given by Mr. Peter Ward of Peat, Marwick and Partners. *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, April 27, 1983, 4:6.

- (10) *R. v. Stewart* (1982), 68 C.C.C. (2d) 305.
- (11) R.S.C. 1970, c. C-30.
- (12) *R. v. McMullen* (1979), 100 D.L.R. (3d) 671.
- (13) *R. v. Bell and Bruce* (1982), 65 C.C.C. (2d) 377.
- (14) *An Act respecting Access to documents held by public bodies and the Protection of personal information*, S.Q. 1982, c. 30.
- (15) Respectively, S.C. 1982, c. 111; and R.S.C. 1970, c. I-5, as amended.
- (16) For greater detail, see *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, May 19, 1983, 10:7.
- (17) *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, May 25, 1983, 12:11.

Appendix "A"

WITNESSES WHO APPEARED BEFORE THE SUB-COMMITTEE

Department of Justice	Date of Appearance
Mr. Norman Hill, Project Chief, Theft and Fraud Project	March 17, 1983
Mr. Neville Avison, Chief, Research and Statistics	March 17, 1983
Royal Canadian Mounted Police	
Superintendent George W. Allen, Commercial Crimes Branch	March 17, 1983
Cerberus Computer Services Inc.	
Mr. James Finch, Toronto	March 23, 1983
Mr. Collin C. Rous, Toronto	March 23, 1983
Canadian Business Equipment Manufacturers Association	
Mr. John Reid, Chairman of the Legislation Committee (CBEMA)	April 19, 1983
Mr. Howard Kaufman, Vice-President of Xerox	April 19, 1983
Mr. John Dean, Senior Legal Advisor of IBM	April 19, 1983
Peat, Marwick and Partners	
Mr. Peter Ward, Toronto	April 27, 1983
University of Western Ontario	
Professor John Palmer, London, Ontario	May 3, 1983
Professor David H. Flaherty, London, Ontario	May 3, 1983
Landspan International of Canada Ltd.	
Mr. Peter J. Lawrence, President/Director	May 10, 1983
Mr. J. Ian Henderson, Vice-President and General Counsel Ottawa, Ontario	May 10, 1983
Mr. Morvin Gentleman, National Research Council	May 11, 1983
Mr. Frank Spitzer, Consultant, Toronto	May 11, 1983
Mr. Dave Conway, Manager, Resources Protection, Mitel Corporation, Kanata, Ontario	May 17, 1983
Professor Tony J. Juliani, Department of Criminology, Ottawa University	May 17, 1983
Professor Grant Hammond, Counsel, Law Center, University of Alberta, Edmonton, Alberta	May 18, 1983
Mr. George E. Fisk, Barrister and Solicitor, Gowling and Henderson, Barristers, Ottawa, Ontario	May 18, 1983
Mr. Paul C. Boire Sr., President, Canadian Association of Data Processing Service Organizations (CADAPSO), Ottawa	May 19, 1983
Mr. D.W. Kay, District Manager, Datacrown Inc., Ottawa	May 19, 1983

Department of Consumer and Corporate Affairs

Mr. Tony Butler, Senior Policy Advisor May 24, 1983

Mr. Bruce Cauchman, Policy Advisor May 24, 1983

Canadian Information Processing Society, Toronto

Mrs. Sally Woodhead, Chairman, Special Interest Group on
Computer Security May 25, 1983

Canadian Bankers' Association

Mr. R.M. MacIntosh, President May 26, 1983

Mr. E. Jestin, Supervisor, Internal Control, Evaluation, The
Bank of Nova Scotia May 26, 1983

Ms. Pat Learmonth, Co-ordinator of Communications May 26, 1983

Consumers' Association of Canada

Ms. Christine Bisanz, Acting Director of Association and
Activities May 31, 1983

Ms. Christine Elliott, Member, Ontario Branch May 31, 1983

Gaston, Snow and Ely Bartlett, Palo Alto, California

Mrs. Susan H. Nycum, Attorney-at-Law June 1, 1983

Canadian Bar Association

Mr. Yves Fortier, President June 8, 1983

Mr. Bernard E. Blanchard, Executive Director June 8, 1983

Ms. Judith Kingston, and June 8, 1983

Mr. Charles W. MacIntosh, Q.C., of the Standing Committee
on Law, Science and Technology June 8, 1983

Mr. Stephen Georgas, Barrister and Solicitor, Toronto June 9, 1983

Department of Justice

Mr. E.A. Tollefson, Co-ordinator, Criminal Code Review June 9, 1983

Mr. Norman Hill, Project Chief, Theft and Fraud Project June 9, 1983

Appendix "B"

SELECTED BIBLIOGRAPHY

The "Selected Bibliography" lists the most important published works that were consulted in the study and preparation of this Report. A more comprehensive list of titles, containing over 300 magazine and scholarly articles, was compiled by the Library of Parliament. This list may be obtained by contacting the Clerk of the House Sub-committee on Computer Crime.

Becker, J., "Rifkin, A Documentary History", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 471-720.

Becker, J., "The Trial of a Computer Crime", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 441-456.

Hammond, G. R., "Quantum Physics, Econometric Models and Property Rights to Information", *McGill Law Journal*, Vol. 27, 1981, 47-72.

Ingraham, D., "On Charging Computer Crime", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 429-439.

Kling, R., "Computer Abuse and Computer Crime as Organization Activities", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 403-427.

Krieger, M., "Current and Proposed Computer Crime Legislation", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 721-771.

Palmer, J. and Resendes, R., Copyright and the Computer, Ministry of Supply and Services Canada, 1982.

Parker, D.B., "Computer Abuse Research Update", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 329-352.

Schjolberg, S., "Computer/Assisted Crime in Scandinavia", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 457-469.

Simkin, M., "Is Computer Crime Important", *Journal of Systems Management*, May 1982, 34-38.

Sokolik, S.L., "Computer Crime - The Need for Deterrent Legislation", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 353-383.

Taber, J.K., "A Survey of Computer Crime Studies", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 275-327.

United States, Department of Justice, Bureau of Justice Statistics, Criminal Justice Resource Manual. Computer Crime, Washington, 1979.

Volgyes, M., "The Investigation, Prosecution and Prevention of Computer Crime: A State-of-the-Art Review", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 385-402.

Watkins, P., "Computer Crime: Separating the Myth From the Reality", *CA Magazine*, Jan. 1981.

Whiteside, T., "The Annals of Crime", *New Yorker*, Aug. 22, 1977, (Pt 1); Aug. 29, 1977 (Pt 2).

A copy of the relevant Minutes of Proceedings and Evidence of the Sub-committee on Computer Crime (Issues Nos. 1 to 17 inclusive and 18 which includes this report) and a copy of the relevant Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs (Issues Nos. 117, 119, 131 and 132) are tabled.

Respectfully submitted,

CLAUDE-ANDRÉ LACHANCE,
Chairman.

MINUTES OF PROCEEDINGS

TUESDAY, JUNE 14, 1983

(20)

[Text]

The Sub-committee on computer crime met *in camera* this day at 3:40 o'clock p.m., the acting Chairman, Mr. Ken Robinson (*Etobicoke—Lakeshore*), presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternate Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

The Sub-committee proceeded to the consideration of the draft report on computer crime.

At 5:30 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

THURSDAY, JUNE 16, 1983

(21)

The Sub-committee on computer crime met *in camera* this day at 5:05 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

The Sub-committee resumed consideration of the draft report on computer crime.

At 6:14 o'clock p.m. the Sub-committee adjourned to the call of the Chair.

The Sub-committee on computer crime met *in camera* this day at 10.01 o'clock a.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

The Sub-committee resumed consideration of the draft report on computer crime.

On motion of Mr. Robinson (*Etobicoke—Lakeshore*), the Third Report of the Sub-committee on computer crime as amended was concurred in.

Ordered,—That the Chairman report the Report to the Standing Committee on Justice and Legal Affairs.

It was agreed,—That the report be printed within turnover format and green special cover.

On motion of Mr. Beatty, it was ordered,—That an additional 2000 copies be printed of Issue No. 18 of the Sub-committee's Minutes of Proceedings and Evidence.

At 12:00 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

Pierre de Champlain
Clerk of the Sub-committee

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à huis clos, à 10h01, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présente: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (Etobicoke—Lake-shore).

Aussi présente: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n°1*).

Le Sous-comité reprend l'étude du projet de rapport sur les infractions relatives aux ordinateurs.

Sur motion de M. Robinson (*Etobicoke—Lakeshore*), le Troisième Rapport du Sous-comité sur les infractions relatives aux ordinateurs, tel que modifié, est adopté.

Il est ordonné,—Que le Président fasse rapport du Rapport au Comité permanent de la justice et des questions juridiques.

Il est convenu,—Que le Rapport soit imprimé en forme tête-bêche avec une couverture spéciale de couleur verte.

Sur motion de M. Beatty, il est ordonné,—Que soient imprimées 2000 copies additionnelles du fascicule n° 18 des procès-verbaux et témoignages du Sous-comité.

A 12h00, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité
Pierre de Champplain

PROCÈS-VERBAL

LE MARDI 14 JUIN 1983

(20)

[Texte]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à huis clos, à 15h40, sous la présidence de M. Ken Robinson (*Etiobicoke—Lakeshore*), président suppléant.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Membres substitués désignés présents: MM. Beatty et Robinson (Etiobicoke—Lakeshore).

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1*).

Le Sous-comité entreprend l'étude du projet de rapport sur les infractions relatives aux ordinateurs.

A 17h30, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

LE JEUDI 16 JUIN 1983

(21)

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à huis clos, à 17h05, sous la présidence de M^{me} Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^{me} Hervieux-Payette.

Aussi présent: M^{me} M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^{er} mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1*).

Le Sous-comité reprend l'étude du projet de rapport sur les infractions relatives aux ordinateurs.

A 18h14, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Taber, J.K., «A Survey of Computer Crime Studies», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 275-327.

Volgyes, M., «The Investigation, Prosecution and Prevention of Computer Crime: A State-of-the-Art Review», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 385-402.

Watkins, P., «Computer Crime: Separating the Myth From the Reality», *CA Magazine*, jan. 1981.

Whiteside, T., «The Annals of Crime», *New Yorker*, le 22 août 1977 (1ère partie); le 29 août 1977 (2e partie).

Un exemplaire des Procès-verbaux et témoignages du Sous-comité sur les infractions relatives aux ordinateurs (fascicules nos 1 à 17 inclusivement et 18 qui comprend le présent rapport) et un exemplaire des Procès-verbaux et témoignages du Comité permanent de la justice et des questions juridiques (fascicules nos 117, 119, 131 et 132) sont déposés.

Respectueusement soumis,

Le président,
CLAUDE-ANDRÉ LACHANCE

Annexe «B»

BIBLIOGRAPHIE SOMMAIRE

Cette «Bibliographie sommaire» contient la liste des principaux articles et ouvrages consultés pendant les travaux et lors de la rédaction du rapport. La Bibliothèque du Parlement a dressé une liste plus complète de plus de 300 titres de revues et d'articles savants. On peut se procurer cette liste en s'adressant au greffier du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs.

Becker, J., «Rifkin, A Documentary History», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 471-720.

Becker, J., «The Trial of a Computer Crime», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 441-456.

Etats-Unis, ministère de la Justice, Bureau of Justice Statistics, Criminal Justice Resource Manual. Computer Crime, Washington, 1979.

Hammond, G. R., «Quantum Physics, Econometric Models and Property Rights to Information», *McGill Law Journal*, vol. 27, 1981, 47-72.

Ingraham, D., «On Charging Computer Crime», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 429-439.

Kling, R., «Computer Abuse and Computer Crime as Organization Activities», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 403-427.

Krieger, M., «Current and Proposed Computer Crime Legislation», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 721-771.

Palmer, J. et Resendes, R., Le droit d'auteur et les ordinateurs, Approvisionnements et Services Canada, 1982.

Parker, D.B., «Computer Abuse Research Update», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 329-352.

Schjolberg, S., «Computer/Assisted Crime in Scandinavia», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 457-469.

Simkin, M., «Is Computer Crime Important?», *Journal of Systems Management*, mai 1982, 34-38.

Sokolik, S.L., «Computer Crime - The Need for Deterrent Legislation», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 353-383.

- M. Grant Hammond, professeur et avocat, Centre d'études juridiques, Université de l'Alberta, Edmonton (Alberta)
Le 18 mai 1983
- Me George E. Fisk, avocat, «Gowling and Henderson Barristers», Ottawa (Ontario)
Le 18 mai 1983
- M. Paul C. Boire Sr., président, l'Association canadienne des entreprises de services en informatique (CADAPSO), Ottawa
Le 19 mai 1983
- M. D.W. Kay, directeur de district, Datacrown Inc., Ottawa
Le 19 mai 1983
- Du ministère de la Consommation et des Corporations:**
- M. Tony Butler, conseiller principal en matière de politiques
Le 24 mai 1983
- M. Bruce Cauchman, conseiller en matière de politiques
Le 24 mai 1983
- De l'Association canadienne de l'informatique, Toronto**
- Mme Sally Woodhead, présidente, Groupe spécial d'intérêt sur la sécurité informatique
Le 25 mai 1983
- De l'Association des banquiers canadiens**
- M. R.M. MacIntosh, président
Le 26 mai 1983
- M. E. Jestin, superviseur, Vérification et évaluation interne, La Banque de Nouvelle-Écosse
Le 26 mai 1983
- Mlle Pat Learmonth, coordinatrice des communications
Le 26 mai 1983
- De l'Association canadienne des consommateurs**
- Mlle Christine Bisanz, directrice suppléante, Politique et activités
Le 31 mai 1983
- Mlle Christine Elliott, membre, section Ontario
Le 31 mai 1983
- De Gaston, Snow and Ely Bartlett, Palo Alto, Californie**
- Mme Susan H. Nycum, avocate
Le 1^{er} juin 1983
- De l'Association du barreau canadien**
- Me Yves Fortier, président
Le 8 juin 1983
- Me Bernard E. Blanchard, directeur général
Le 8 juin 1983
- Me Judith Kingston et
Le 8 juin 1983
- Me Charles W. MacIntosh, c.r., du Comité permanent du droit, des sciences et de la technologie
Le 8 juin 1983
- Me Stephen Georgas, avocat, Toronto
Le 9 juin 1983
- Du ministère de la Justice:**
- M. E.A. Tollefson, coordonnateur, Révision du Code criminel
Le 9 juin 1983
- M. Norman Hill, chef de projet, Projet de vol et fraude
Le 9 juin 1983

Annexe «A»

TÉMOINS QUI ONT COMPARU DEVANT LE SOUS-COMITÉ

Date de la comparu-
tion

Du ministère de la Justice

M. Norman Hill, chef de projet, Projet vol et fraude
Le 17 mars 1983

M. Neville Avison, chef, Recherche et statistiques
Le 17 mars 1983

De la Gendarmerie royale du Canada

Surintendant George W. Allen, Section des délits commerciaux
Le 23 mars 1983

De Cerberus Computer Services Inc.

M. James Finch, Toronto
Le 23 mars 1983

M. Collin C. Rous, Toronto
Le 23 mars 1983

De l'Association canadienne des fabricants d'équipement de bureau

M. John Reid, président du Comité de la législation (ACFEB)
Le avril 19 1983

M. Howard Kaufman, vice-président, Xerox
Le avril 19 1983

M. John Dean, conseiller juridique principal, IBM
Le avril 19 1983

De Peat, Marwick and Partners

M. Peter Ward, Toronto
Le avril 27 1983

De l'Université Western, Ontario

M. John Palmer, professeur, London (Ontario)
Le 3 mai 1983

M. David H. Flaherty, professeur, London (Ontario)
Le 3 mai 1983

De Landspan International of Canada Ltd.

M. Peter J. Lawrence, président-directeur
Le 10 mai 1983

M. J. Ian Henderson, vice-président et avocat-conseil général,
Ottawa (Ontario)
Le 10 mai 1983

M. Morvin Gentleman, Conseil national de recherches
Le 11 mai 1983

M. Frank Spitzer, expert-conseil, Toronto
Le 11 mai 1983

M. Dave M. Conway, directeur, Protection des ressources, Mittel
Corporation, Kanata (Ontario)
Le 17 mai 1983

M. Tony J. Juliani, professeur, Département de Criminologie,
Université d'Ottawa
Le 17 mai 1983

- (10) *R. c. Stewart* (1982), 68 C.C.C. (2d) 305.
- (11) S.R.C. 1970, c. C-30.
- (12) *R. c. McMullen* (1979), 100 D.L.R. (3d) 671.
- (13) *R. c. Bell and Bruce* (1982), 65 C.C.C. (2d) 377.
- (14) *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, S.Q. 1982, c. 30.
- (15) S.C. 1982, c. 111 et S.R.C. 1970, c. I-5 modifié, respectivement.
- (16) Voir les *Procès-verbaux et témoignages* du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 19 mai 1983, 10:7.
- (17) Voir les *Procès-verbaux et témoignages* du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 25 mai 1983, 12:11.

- (1) La liste des témoins qui ont comparu devant le Sous-comité se trouve à l'Annexe «A».
- (2) Le premier ordinateur, l'ENIAC (intégrateur et calculateur électronique numérique), a vu le jour en 1946 à l'Université de Pennsylvanie. Pour de plus amples détails, voir S. Sokolik, «The Computer Crime—The Need for Deterrent Legislation», *Computer/Law Journal*, vol. II, no 2, printemps 1980, pp. 353-385 (p. 354).
- (3) *Security World*, janvier 1982, p. 28.
- (4) Témoignage présenté par M. Peter Ward, de Peat, Marwick and Partners. Voir les procès-verbaux et témoignages du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 27 avril 1983, 4:18.
- (5) S.R.C. 1970, c. C-34.
- (6) *R. c. Christensen et al.* (1978), 26 *Chitty's Law Journal*, p. 348 (Cour suprême de l'Alberta, Division de première instance).
- (7) *McLaughlin c. R.* (1979), 12 C.R. (3d) 391 (Cour d'appel de l'Alberta); et *Sa Majesté la Reine c. McLaughlin* (1980) 2 R.C.S. 331 (Cour suprême du Canada).
- (8) Cette enquête de la Sûreté provinciale de l'Ontario, intitulée «Sondage sur la criminalité et la sécurité informatiques», a été présentée par le Surintendant G.W. Allen, de la Section des délits commerciaux de la G.R.C., qui a comparu devant le Sous-comité le 17 mars 1983.
- (9) Témoignage présenté par M. Peter Ward, de Peat, Marwick and Partners. Voir les *Procès-verbaux et témoignages* du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 27 avril 1983, 4:6.

NOTES

70. Conformément au paragraphe (13) de l'article 69 du *Règlement de la Chambre des communes, articles permanents et provisoires*, le Comité permanent de la justice et des questions juridiques demande au gouvernement de déposer une réponse globale dans les 120 jours suivant le dépôt du présent rapport à la Chambre des communes.

DEMANDE CONFORMÈMENT AU PARAGRAPHE (13) DE L'ARTICLE 69 DU RÈGLEMENT DE LA CHAMBRE DES COMMUNES

69. Il est par conséquent nécessaire d'améliorer les recours afin d'offrir aux victimes des délits informatiques la forme de réparation la plus appropriée. Cependant, ces mesures n'entrent en jeu qu'une fois le délit commis. À notre avis, il est plus important de veiller à ce que toutes les mesures préventives possibles soient soigneusement appliquées. Si les systèmes informatiques sont bien protégés et si leurs usagers sont convenablement formés, on pourra prévenir un bon nombre d'actes répréhensibles qui seraient autrement commis.

68. Dès le début de ses travaux, le Sous-comité s'est rendu compte qu'il était impossible de séparer la criminalité informatique de l'«information» en général. Pour cette raison, nous avons fait des recommandations qui pourraient facilement dépasser notre mandat, limité à la criminalité informatique et au droit pénal. Nous estimons cependant qu'il est souhaitable de prévoir tous les recours possibles, la modification du *Code criminel* n'étant qu'une solution parmi tant d'autres. Quant à l'effet de dissuasion, la possibilité de poursuivre en dommages et intérêts les auteurs de délits informatiques peut être aussi efficace que l'imposition d'une amende ou d'une peine de prison.

CONCLUSION

67. Le Sous-comité considère donc qu'il serait très utile d'inclure des notions d'éthique dans tout programme de formation en informatique. L'enseignement de valeurs morales aux usagers, dès le début, est peut-être un autre moyen de combattre la criminalité informatique. Le Sous-comité recommande par conséquent que les professeurs d'informatique soient tenus d'être qualifiés dans le domaine de l'éthique en informatique et que les responsabilités morales liées à l'utilisation d'ordinateurs figurent dans les cours d'informatique de tous les niveaux.

66. On se rend de plus en plus compte que les usagers des systèmes informatiques ne sont pas toujours conscients de leurs responsabilités sur le plan de l'éthique. Le problème est particulièrement notable chez les adolescents et les jeunes étudiants dont la maturité d'esprit est parfois beaucoup moins développée que leurs connaissances en informatique.

65. Le Sous-comité appuie ces efforts qui dissuaderont peut-être les auteurs de délits en puissance et inculqueront des principes d'éthique aux usagers des ordinateurs. Si l'industrie ne se réglemente pas elle-même, il se pourrait bien que des mécanismes d'accréditation obligatoire ou d'octroi de permis doivent être envisagés plus tard, mais la situation actuelle ne justifie cependant pas de mesures de ce genre. Le Sous-comité recommande par conséquent que l'industrie de l'informatique adopte ses propres règlements pour veiller à ce que ses membres aient une conduite irréprochable.

64. L'Association canadienne de l'informatique (ACI) est en train d'établir un processus d'accréditation des programmeurs de systèmes afin que l'industrie puisse réglementer ses propres membres. Ce processus est encore loin d'être terminé. (17)

63. L'industrie de l'informatique étant relativement nouvelle, il y existe très peu de mesures destinées à régir les activités des personnes qui travaillent avec des ordinateurs. Bien que l'information contenue dans ces ordinateurs ait souvent une valeur inestimable ou un contenu confidentiel, il n'y a dans ce domaine aucun code de déontologie obligatoire comme c'est le cas dans d'autres disciplines, par exemple le droit et la médecine. L'Association canadienne des entreprises de services en informatique (CADAPSO) a établi un code d'éthique exposant des normes de comportement dans l'intérêt public et des dispositions sur les relations avec les non-membres assurant des services de traitement des données (16). Il n'est cependant pas nécessaire d'être membre de la CADAPSO pour assurer des services en informatique.

3. Code d'éthique

62. Il existe dans d'autres lois fédérales et provinciales certaines dispositions sur la confidentialité des renseignements à caractère personnel, par exemple, au niveau fédéral, les articles 62 et 63 de la *Loi sur la protection des renseignements personnels* et l'article 241 de la *Loi de l'impôt sur le revenu* (15), mais aucune loi globale sur le sujet n'a jamais été adoptée. À notre avis, il y aurait lieu d'étudier plus en profondeur cet aspect peu développé de la législation.

61. La loi québécoise est fondée sur le principe que toute information détenue par le secteur public doit être considérée comme confidentielle à moins que la personne concernée n'autorise sa divulgation. Le gouvernement peut adopter des règlements fixant des normes de sécurité destinées à veiller à ce que cette information demeure confidentielle. Par ailleurs, des peines sont prévues pour toute divulgation illégale de données à caractère personnel détenues par le secteur public.

d'une loi innovatrice sur l'accès aux documents publics et la protection des données à caractère personnel. (14)

60. La protection de la vie privée relève dans une large mesure des autorités provinciales, mais aucune province n'a encore pris l'initiative d'adopter des mesures législatives générales pour protéger toutes les données à caractère personnel, sauf le Québec, qui s'est doté

59. Étant donné les extraordinaires possibilités de l'ordinateur dans les domaines de la collecte et du traitement de données, bien des gens s'inquiètent de la menace que l'ordinateur pourrait constituer pour les données confidentielles à caractère personnel. Les défenseurs de la vie privée ont même recommandé de tenir criminellement responsables les personnes préposées à la garde de données à caractère personnel dans le cas où quelqu'un obtiendrait illegalement accès à ces données en raison de l'insuffisance des mesures de sécurité. Le Sous-comité comprend leur inquiétude, mais il ne peut pour le moment appuyer des mesures aussi draconiennes. Cependant, il faudrait prendre des dispositions pour que les données à caractère personnel, qu'elles soient stockées ou non dans un ordinateur, soient suffisamment protégées de tous ceux qui n'ont pas le droit d'y avoir accès.

58. Le Sous-comité considère que le droit relatif au secret industriel pourrait être considérablement amélioré pour offrir une meilleure protection à toutes les personnes dont les secrets ont été violés, que ce soit par des moyens informatiques ou autrement; les pertes dues aux vols de secrets industriels peuvent en effet être considérables. À l'heure actuelle, cette question relève des provinces, et aucune d'entre elles n'a encore adopté de loi sur le sujet. Il se pourrait qu'il soit nécessaire plus tard de faire du vol de secrets industriels un acte criminel. Le Sous-comité recommande néanmoins aux gouvernements fédéral et provinciaux d'étudier à fond, conjointement, le droit relatif au secret industriel et d'adopter les mesures correctives qui s'imposent.

57. Le droit relatif au secret industriel est aussi peu précis que celui qui se rapporte aux monopoles légaux du gouvernement fédéral. À l'heure actuelle, la protection du secret industriel, qui n'est prévue qu'en *common law*, est assez efficace lorsqu'il existe clairement un lien *confidentiel* entre deux parties, par exemple dans le cas d'un employé tenu de garder secrète une information reçue dans l'exercice de ses fonctions. Cette protection est cependant moins bien définie lorsque des secrets industriels sont communiqués à une tierce partie qui ne s'était pas engagée à l'origine à garder le secret.

56. Les dispositions sur les brevets et les dessins industriels peuvent elles aussi offrir des possibilités pour la protection des programmes informatiques. En raison du petit nombre de témoignages entendus à ce sujet, le Sous-comité a décidé de ne pas se prononcer sur la question pour le moment. Nous recommandons cependant que le gouvernement fédéral effectue une étude en profondeur sur la possibilité d'étendre aux programmes informatiques la protection visant les brevets et les dessins industriels.

55. Le Sous-comité tient à souligner qu'au Canada, la révision de la *Loi sur le droit d'auteur* en est actuellement à sa dernière étape. Convaincus que les victimes des délits informatiques devraient avoir autant de possibilités de recours que possible, nous estimons que la protection par le droit d'auteur devrait être étendue aux logiciels informatiques. Nous recommandons par conséquent de modifier la Loi sur le droit d'auteur pour y inclure les logiciels informatiques.

sur le sujet afin d'y inclure les logiciels informatiques après qu'un comité présidentiel eut longuement étudié l'application du droit d'auteur aux techniques de pointe.

54. Les logiciels informatiques ne figurent pas expressément au nombre des oeuvres protégées par l'actuelle *Loi sur le droit d'auteur*. Dans la pratique, bon nombre de créateurs demandent cette protection pour leurs programmes mais la loi n'est pas claire à ce sujet. Un certain nombre de spécialistes de la question nous ont affirmé que, selon eux, le droit d'auteur est le meilleur moyen de protection. En 1978, les Etats-Unis ont modifié leurs lois

53. Au niveau fédéral, les dispositions relatives aux monopoles légaux visant le droit d'auteur, les brevets, les dessins industriels, et les marques de commerce sont les seuls recours au civil. Les lois sur le droit d'auteur et sur les brevets semblent les plus susceptibles d'être utiles aux victimes de délits relatifs à des logiciels informatiques. L'opinion semble cependant favoriser la protection par le droit d'auteur.

52. Les recours au civil constituent un complément important aux dispositions du droit pénal. Dans de nombreux cas, les victimes de délits informatiques ne tiennent pas particulièrement à ce que les auteurs de ces délits soient poursuivis au criminel, préférant tenter une action civile afin d'être indemnisés de leurs pertes. Par exemple, si quelqu'un vole un programme de jeu vidéo et vend ensuite des jeux pirates, le créateur du programme peut préférer être indemnisé, plutôt que d'envoyer le voleur en prison. Cette dernière solution n'apporterait en effet pas grand-chose à une victime que cet acte de «piraterie» aurait mis au bord de la faillite.

2. Recours au civil

51. Le Sous-comité ne recommande pas, pour le moment, de normes de sécurité obligatoires, bien que certains témoins l'aient proposé. Il se pourrait bien que la nécessité d'adopter des règlements en ce sens s'impose d'elle-même plus tard. En attendant, nous recommandons que l'industrie de l'informatique et les organismes usagers évaluent les faiblesses de leurs systèmes et adoptent les mesures de sécurité nécessaires.

50. Selon les témoignages entendus au cours des audiences, il semble que bon nombre des délits informatiques auraient pu être évités si des mesures de sécurité efficaces avaient été appliquées. Il est évident que l'industrie doit adopter ses propres règlements. Selon nous, tous les systèmes informatiques dans lesquels sont stockées des données ayant une certaine valeur, du point de vue commercial ou personnel, doivent respecter des normes de sécurité adéquates.

49. Comme nous l'avons déjà souligné, le Sous-comité est fermement convaincu que le droit pénal ne doit constituer qu'une des solutions possibles au problème de la criminalité informatique. Parmi toutes les autres options qui nous ont été présentées, nous estimons que les plus importantes sont celles qui touchent les mesures de sécurité.

1. Normes de sécurité

G. Mesures supplémentaires

auteurs ait une connaissance suffisante du domaine. Les systèmes informatiques sont en effet très complexes, et les néophytes sont facilement dépassés. Le Sous-comité recommande par conséquent de faire tous les efforts possibles pour veiller à ce que les policiers et les avocats de la Couronne qui pourraient être amenés à s'occuper de criminalité informatique reçoivent une formation leur permettant de s'acquitter efficacement de leurs fonctions.

48. Il ne suffit toutefois pas d'améliorer les techniques d'application de la loi et les pouvoirs connexes pour résoudre efficacement le problème de la criminalité informatique. Il faut aussi que le personnel chargé de détecter les délits informatiques et de poursuivre leurs

47. Le Sous-comité recommande par conséquent d'étudier à fond toutes les questions liées à la détection des délits informatiques et aux poursuites contre leurs auteurs, particulièrement en ce qui concerne l'étendue des pouvoirs de perquisition et de saisie, ainsi que les lois fédérales et les traités portant sur les enquêtes internationales et l'extradition; il y aurait lieu également d'étudier l'application, aux communications entre ordinateurs, des dispositions du *Code criminel* en matière d'écoute électronique.

46. Par leur nature même, les délits informatiques sont difficiles à détecter. Selon les témoignages présentés au Sous-comité, il semble que dans bien des cas, leur découverte soit purement et simplement une question de chance. Puisqu'il est à ce point complexe de détecter les délits informatiques, de recueillir des preuves et de poursuivre les auteurs de ces délits, particulièrement dans le cas du transfert transfrontalier de données, il est essentiel de perfectionner les procédures permettant de le faire.

F. Les problèmes d'application de la loi

45. Le Sous-comité a entendu très peu de témoignages sur cet aspect de son mandat. Le 18 novembre 1982, le gouvernement a déposé le projet de loi S-33, intitulé «Loi donnant effet pour le Canada à la Loi uniforme sur la preuve adoptée par la Conférence canadienne de l'uniformisation du droit». Ce projet de loi, qui traite notamment de l'admissibilité des imprimés d'ordinateur, est devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles. Nous n'avons donc pas l'intention de faire de recommandations précises: nous sommes en effet convaincus que les problèmes que nous étudions avec toute l'attention qu'ils méritent. Nous ne nous néanmois à souligner l'importance des travaux du Comité sénatorial.

44. Depuis le jugement *Bell and Bruce*, les difficultés soulevées par l'affaire *McMullen* semblent s'être résolues d'elles-mêmes dans la pratique, bien que les juristes ne s'entendent pas encore sur l'importance à accorder au jugement *Bell and Bruce* par rapport au jugement *McMullen*.

43. L'affaire *McMullen* semble être passée au second plan lorsqu'un jugement a été rendu dans l'affaire *R. c. Bell and Bruce*. (13) Dans cette affaire, le juge a décidé que les imprimés d'ordinateur constituent des «registres», au sens où l'entend le paragraphe 29(2) de la *Loi sur la preuve au Canada*, puisque ce sont les seules sources de référence dont les banques disposent pour connaître l'état de leurs comptes. À titre de «registres», au sens où l'entend le paragraphe 29(2), les imprimés d'ordinateur ont donc été jugés admissibles sur la foi d'une déclaration sous serment.

42. Ce jugement n'a pas été très bien reçu, particulièrement au sein des institutions financières. Non seulement permettait-il l'introduction de preuves susceptibles de nuire à la sécurité de leurs installations informatiques, puisqu'il exigeait la description des procédures à suivre, mais il obligeait en outre trop d'employés de banque à s'absenter du travail pour témoigner.

41. Cette modification semble avoir été proposée en réponse à l'affaire *R. c. McMullen*. (12) Dans cette cause, qui date de 1979, la Cour a statué que, pour que des imprimés d'ordinateur soient recevables, l'ensemble de la preuve doit refléter tout le processus de tenue des dossiers (c'est-à-dire, dans le cas des imprimés d'ordinateur, toutes les procédures à suivre pour l'introduction, le stockage, l'extraction et la présentation de l'information), et que si les gestionnaires, les comptables ou le personnel chargés des dossiers en cause étaient incapables de produire cette preuve, les imprimés d'ordinateur n'étaient pas admissibles.

40. Le Sous-comité avait notamment pour mandat d'étudier la possibilité de modifier la *Loi sur la preuve au Canada*. L'article 6 du projet de loi C-667 propose en effet de modifier cette loi de façon que les états mécanographiés (imprimés d'ordinateur) soient admissibles en preuve au même titre que les documents originaux.

F. La Loi sur la preuve au Canada

39. Comme nous l'avons déjà souligné, on connaît très mal l'ampleur du problème de la criminalité informatique. Afin de corriger cet état de choses, certains proposent d'adopter des dispositions législatives obligeant à signaler ces délits. Le Sous-comité n'est pas en faveur de cette approche. Le *Code criminel* ne comprend guère de dispositions de ce genre, même pour les crimes les plus graves comme l'homicide. Il serait donc selon nous injustifiable que la loi oblige à signaler les délits informatiques si elle ne l'exige pas pour la plupart des autres infractions. Par ailleurs, il serait malaisé d'adopter une disposition de ce genre car il serait très difficile de la faire respecter.

38. Le Sous-comité ne tient à aucune formulation particulière. Cependant, nous avons été mis en garde à maintes reprises contre le danger qu'il y aurait à établir des définitions à partir des techniques actuelles. En effet, les progrès étant extrêmement rapides dans le domaine de l'informatique, il est essentiel d'éviter les termes techniques susceptibles d'être rapidement dépassés. Nous recommandons donc que les définitions nécessaires à la description des diverses infractions portent le plus possible sur les fonctions exécutées et non sur les techniques en cause.

37. Le Sous-comité recommande par conséquent de modifier le *Code criminel* afin de créer deux nouvelles infractions: l'utilisation non autorisée d'un système informatique (sans apparence de droit) et la modification ou la destruction non autorisées (sans apparence de droit) de données informatisées. Le Sous-comité recommande en outre que les avocats de la Couronne aient le choix entre la déclaration sommaire de culpabilité et l'inculpation.

36. Le Sous-comité n'est pas en faveur de cette dernière proposition. Selon lui, les questions d'ordre pratique doivent passer après les exigences de précision et d'équité du droit pénal. À notre avis, la différence entre les deux genres d'actes est trop grande pour qu'ils puissent être traités sur la foi d'une même preuve.

35. Globalement, le Sous-comité est favorable à cette approche. On pourrait néanmoins soutenir qu'il existerait déjà un délit simple «d'utilisation non autorisée» et qu'il serait possible de tenir compte de la gravité de l'infraction en donnant le choix entre l'inculpation et la déclaration sommaire de culpabilité, et en prévoyant une vaste gamme de peines.

accordés se rapprochent davantage d'un droit d'exploitation valable pendant une période limitée. Par exemple, en vertu de la *Loi sur le droit d'auteur*(1), l'auteur d'un livre a le droit exclusif de «produire ou reproduire» son livre. Par contre, rien n'empêche d'autres personnes de s'en inspirer. Il est simplement interdit d'en faire des copies ou de le plagier, car il s'agit là d'un droit exclusif de l'auteur et de ses cessionnaires, et ce pendant la vie de l'auteur, plus une période de 50 ans après sa mort. Des considérations analogues quoique pas tout à fait identiques entrent en jeu en ce qui concerne les autres monopoles prévus dans la loi. Pour ces raisons, nous pensons que l'extension de la définition de «bien» afin d'englober «l'information» pourrait entraîner davantage de problèmes qu'elle n'en résoudrait.

31. Deuxièmement, cette mesure est à déconseiller parce qu'elle conférerait à l'information stockée sur ordinateur un statut différent de l'information consignée par des méthodes classiques. Nous ne sommes pas convaincus que la nature du stockage doit influencer sur la protection juridique accordée. Des renseignements prélevés dans un classeur ou un ordinateur sont des renseignements volés. À notre avis, par souci de logique, toutes les informations doivent être traitées de façon uniforme, quel qu'en soit le support.

32. Il serait également possible d'élaborer une loi entièrement distincte qui porterait sur toutes les questions liées à l'informatique. Cette possibilité, qui n'a été recommandée par aucun des témoins qui ont comparu devant nous, pose des problèmes pour plusieurs raisons. D'abord, l'élaboration d'une loi satisfaisante nécessiterait beaucoup plus de temps et un surcroît de travail pour en arriver à une bonne vue d'ensemble de la situation. À notre avis, il est plus important d'introduire des modifications restreintes que d'attendre l'élaboration d'une loi générale. Deuxièmement, pour les raisons précitées, il serait peu souhaitable de traiter les délits informatiques différemment des autres actes criminels. Si l'acte en question est de nature criminelle, il doit logiquement relever du *Code criminel*. Enfin, le Parlement n'a probablement pas la compétence législative nécessaire pour adopter une telle loi, étant donné les conflits possibles avec les domaines de compétence provinciale en matière législative.

33. L'idée la plus répandue chez les témoins consistait à ajouter des dispositions distinctes au *Code criminel* pour protéger spécifiquement l'intégrité des ordinateurs. Une de ces dispositions définirait comme un acte criminel le fait d'utiliser un système informatique sans autorisation. Dans une proposition soumise au Sous-comité, l'Association du barreau canadien suggère le libellé suivant: «Quiconque, sans apparence de droit, utilise un système informatique ou une partie d'un tel système sans l'autorisation du propriétaire» comme un acte criminel. D'autres variantes ont été proposées, bien qu'elles n'aient pas été rédigées sous la forme d'articles de loi. Il s'agirait de considérer comme une infraction le fait d'entraver le fonctionnement d'un ordinateur sans autorisation légitime, d'utiliser illégalement un ordinateur, de prendre des données sans autorisation ou d'obtenir des services informatiques sans autorisation.

34. Un certain nombre de témoins ont recommandé de créer une deuxième infraction afin d'interdire les actes plus répréhensibles consistant à modifier des données après avoir obtenu accès à l'ordinateur. À cet égard, l'Association du barreau canadien recommande que l'on définisse une autre infraction qui serait le délit commis par «quiconque, sans apparence de droit, modifie ou détruit des programmes ou des logiciels informatiques sans l'autorisation du propriétaire». Cette formulation, qui vise la question de la modification ou de la destruction de données, reflète assez bien les vues de ceux qui sont en faveur de la création d'une infraction additionnelle.

phone. Cette liste mécanographique devait apparemment être utilisée pour syndiquer les employés de l'hôtel.

25. En première instance, le juge n'a pas retenu les arguments de la Couronne soutenant que l'expression «quelque chose», qu'il s'agisse de quelque chose de tangible ou d'intangible, utilisée dans l'article 283 du *Code criminel* sur le vol, devait représenter «quelque chose» pouvant être considéré comme un bien. Des renseignements confidentiels comme une liste d'employés ne sont pas considérés comme un bien aux fins de la loi sur le vol. Quiconque se contente de prendre ou de falsifier des données confidentielles ne prend ni ne falsifie «quelque chose» en vertu de l'article 283.

26. Étant donné que la Cour suprême du Canada a éliminé la possibilité d'assimiler les ordinateurs à des installations de télécommunication, toutes sortes d'activités constituant une violation de systèmes informatiques ne sont pas prosrites.

27. Ces actes repérhensibles qui ne sont pas interdits par le *Code criminel* englobent des activités fort diverses. Celles-ci vont des frasques relativement sans conséquences de plaintes qui s'amusent à s'immiscer dans les banques de données des autres ou à les découvrir sans intention de modifier ou de détruire les données, jusqu'à l'espionnage industriel, plus grave et plus complexe, où un concurrent copie, sans laisser de traces, des renseignements stockés sur ordinateur qui non seulement sont confidentiels, mais ont une grande valeur, par exemple des données sur d'importants projets de mise en valeur de terrains ou sur de nouvelles découvertes de pétrole. Même si l'information en soi n'a aucune valeur monétaire, les risques de dommages peuvent être élevés. Par exemple, un individu sans scrupules pourrait obtenir accès à des fichiers informatiques sur des employés et utiliser ces renseignements à des fins impropres.

28. Quelle que soit la gravité des actes en question, le Sous-comité estime qu'il faut prévoir des sanctions pénales pour les réprimer, opinion généralement partagée par tous les témoins qui ont comparu devant lui. Néanmoins, on ne s'entend pas vraiment sur la nature exacte de la réforme nécessaire.

D. Le droit pénal: modifications proposées

29. Selon certains témoins, la définition du terme «bien» devrait être étendue afin d'englober «l'information» ou «l'information stockée sur ordinateur», de telle sorte que les dispositions actuelles du *Code criminel* puissent s'appliquer. Le Sous-comité conteste cette approche. À son avis, il serait malavisé d'assortir de droits de propriété l'information en tant que telle, car cette notion n'existe même pas dans le droit civil. Pour des raisons de politique publique, la propriété exclusive de l'information qui découlerait nécessairement de l'application, aux données, de la notion de «bien», s'inscrit mal dans notre système socio-juridique. L'information est considérée comme un bien public trop important pour qu'on en fasse la propriété exclusive de quiconque.

30. Même dans la législation relative aux droits d'auteur, aux brevets, aux marques de commerce et aux dessins industriels, l'inventeur, le créateur ou le concepteur de l'oeuvre n'a pas de droits de propriété exclusifs sur sa création, son invention ou son dessin. Les droits

l'infraction, et non d'accessoire. Selon d'autres sources, 75 cas approximativement sont signalés tous les ans à l'échelle mondiale, représentant des pertes annuelles d'environ 40 millions de dollars.(9)

19. Ces témoignages contredisent catégoriquement la théorie de la «pointe de l'iceberg» selon laquelle 85% de tous les délits informatiques ne sont jamais signalés et représentent des pertes annuelles approximatives de milliards de dollars. Les témoignages entendus par le Sous-comité ne permettent pas d'étayer cette estimation. Il est sans doute plus sûr de conclure que la fréquence réelle des délits informatiques est tout simplement inconnue. Aucune étude exhaustive n'a jamais été effectuée au Canada pour l'estimer, et nous ne pensons pas que cela soit nécessaire pour le moment. À notre avis, le manque relatif d'informations sur la fréquence et la gravité des délits informatiques ne justifie pas l'action sur le plan législatif. Il faut quand même se préoccuper de leurs conséquences destructrices pour la société et prendre des mesures législatives pour interdire les actes répréhensibles et décourager les fraudeurs.

C. Le droit pénal: situation actuelle

20. Sur le plan théorique, on peut aborder la question de la criminalité informatique en établissant une distinction entre la notion d'ordinateur comme instrument du délit et la notion d'ordinateur comme objet du délit.

21. Dans la première catégorie, l'ordinateur est utilisé pour commettre l'infraction. L'infraction elle-même n'est pas nouvelle; seul le moyen utilisé pour la commettre l'est. Les plus importantes infractions tombant dans cette catégorie sont les fraudes réalisées au moyen d'un ordinateur: il s'agit d'infractions pour lesquelles des poursuites ont été intentées avec succès par l'application des dispositions actuelles du *Code criminel*.

22. La deuxième catégorie, où l'ordinateur est l'objet du délit, n'est pas si précise. Elle englobe les délits «matériels», où des dommages tangibles sont causés à un ordinateur ou à ses éléments, ou bien lorsqu'il y a vol de ceux-ci. Cette catégorie comprend le vol et le méfait classiques. Les contrevenants sont facilement poursuivis en vertu des mesures législatives actuelles.

23. Le vrai problème se pose lorsque l'ordinateur, en tant qu'objet du délit, n'est victime d'aucun dommage tangible, comme ce fut le cas dans l'affaire *McLaughlin*. On se souviendra que *McLaughlin* a été acquitté de l'inculpation de méfait parce que les preuves étaient insuffisantes pour établir sa responsabilité dans les pannes de l'ordinateur. Si rien ne vient gêner le fonctionnement ou l'exploitation légitimes de l'ordinateur, ou l'utilisation de l'ordinateur par ses usagers autorisés, il y a peu de chances d'obtenir une condamnation en vertu des dispositions du *Code criminel* sur le méfait.

24. On a tenté récemment d'appliquer à ce genre d'activité les dispositions générales du Code criminel sur le vol. Dans l'affaire *R. c. Stewart*(10), la Couronne a soutenu que l'inculpé était coupable d'avoir conseillé le vol de données appartenant à un hôtel, le plaissant, parce que l'inculpé avait tenté d'obtenir d'un employé de l'hôtel une copie de la liste mécanographique des employés contenant leur nom, leur adresse et leur numéro de téléphone.

18. Les représentants de l'Association des banquiers canadiens ont témoigné qu'à leur connaissance, aucun des membres de leur Association n'a jamais été victime d'un délit informatique «pur», c'est-à-dire d'un délit où l'ordinateur a servi de moyen de perpétration de

17. Il existe très peu de données empiriques prouvant de façon probante que la criminalité informatique constitue un grave problème. La Sûreté provinciale de l'Ontario a effectué une enquête auprès de 648 sociétés entre 1980 et 1981. Sur 321 répondants, seulement 13 ont signalé des pertes par délit informatique. Il s'agissait dans les deux tiers des cas de vols de temps-machine et de dommages volontaires à des fichiers ou à du matériel informatique. Seulement cinq cas ont été signalés à la police à l'époque, et uniquement trois poursuites semblent avoir été intentées.(8)

16. La fréquence des délits informatiques est aussi assez mal connue parce que certains délits passent parfois inaperçus ou, s'ils sont découverts, parce qu'ils ne sont pas signalés étant donné que les victimes, particulièrement dans le monde des affaires, préfèrent parfois éviter toute publicité négative. Il arrive également que les victimes estiment que le problème peut être le mieux réglé au niveau interne ou que les pertes subies sont simplement trop faibles pour justifier la prise de mesures importantes.

15. La fréquence des délits informatiques est difficile à estimer. Certains chiffres sont quelque peu excessifs parce que n'importe quel acte répréhensible associé de loin avec un ordinateur est souvent qualifié de délit informatique. Par exemple, si un employé de banque malhonnête falsifie manuellement des documents financiers qui sont par la suite stockés dans l'ordinateur de la banque, cette forme de détournement de fonds n'est plus appelée une fraude. Au lieu de cela, on considère qu'il y a délit informatique, quel que soit le rôle de l'ordinateur dans la perpétration de l'infraction. De la même façon, lorsqu'une personne obtient frauduleusement des fonds d'un guichet de banque automatique grâce au vol d'une carte de crédit et à l'obtention frauduleuse du mot de passe correspondant, cette infraction est une fois encore décrite comme un délit informatique, et non comme le simple vol d'une carte de crédit. Autrement dit, on a généralement tendance à conférer un caractère sensationnel à des infractions par ailleurs assez communes.

B. Fréquence des délits informatiques

14. Il y a lieu de préciser ici que l'expression «criminalité informatique» est impropre. Elle a l'avantage d'être brève, mais il serait plus approprié de parler de délits «liés à l'informatique». De plus, étant donné que tout acte anti-social considéré comme criminel par nature ne constitue pas un «acte criminel» au Canada à moins qu'il ne soit interdit par la loi, il s'ensuit qu'il serait plus approprié d'utiliser des expressions comme «actes répréhensibles associés à l'informatique» ou «actes répréhensibles liés à l'informatique». En fait, le Sous-comité a pour mandat de proposer des modifications au *Code criminel* afin que les «actes répréhensibles liés à l'informatique» qui ne sont pas proscrits actuellement deviennent des actes criminels. Cela dit, nous emploierons dans le reste de ce rapport les expressions «criminalité informatique» et «délict informatique» par souci de simplicité, que l'acte répréhensible en question constitue ou non un acte criminel.

méthode était simple. Grâce à un répertoire de numéros de téléphone d'ordinateurs, ces élèves ont réussi à se brancher sur les ordinateurs canadiens et à s'immiscer dans le réseau tout simplement en essayant tour à tour différents mots de passe jusqu'à ce que l'un d'eux fonctionne. Ils ont fait 21 tentatives de pénétration dans des systèmes informatiques canadiens, mais elles n'ont pas toutes réussi. Certains systèmes étaient très bien protégés au moyen de contrôles et de codes perfectionnés. Deux entreprises seulement ont révélé que leurs banques de données avaient été infiltrées et que des informations y avaient été détruites.

10. Le deuxième cas s'est produit à l'Université de l'Alberta. Pendant l'été 1977, l'ordinateur de l'université a été victime de pannes inhabituellement fréquentes. Soupçonnant une irrégularité, le personnel de l'université a exercé une étroite surveillance et a fini par prendre sur le fait un élève d'école secondaire qui utilisait le système informatique à partir de l'un des terminaux situés sur le campus. L'élève en question n'était pas autorisé à utiliser l'ordinateur. Il a été accusé de méfait en vertu de l'alinéa 287(1)c) du Code criminel(5) et d'utilisation illégale d'une installation de télécommunication en vertu de l'alinéa 287(1)b). Deux autres suspects ont également été accusés de complicité, en vertu du paragraphe 21(1) du Code criminel.

11. Lors du procès, un des inculpés a été acquitté faute de preuves suffisantes. Le deuxième, l'élève d'école secondaire pris sur le fait, a été reconnu coupable de deux chefs d'accusation. Le troisième, qui s'appelaient McLaughlin, a été reconnu coupable du deuxième chef d'accusation, mais il a été acquitté de l'accusation de méfait étant donné que les preuves réunies n'ont pas permis d'établir sa responsabilité dans les pannes de l'ordinateur.(6) McLaughlin a interjeté appel de son unique condamnation. Dans une décision rendue à deux contre un, la Cour d'appel de l'Alberta a accueilli l'appel et a infirmé la déclaration de culpabilité arguant qu'un système informatique ne constitue pas une «installation de télécommunication». Cette décision a été entérinée par la Cour suprême du Canada.(7)

12. L'affaire McLaughlin est importante car elle a révélé que certaines activités, qui seraient autrement considérées comme des infractions, ne constituent pas un acte criminel tout simplement parce que les dispositions actuelles du Code criminel présentent des lacunes. Étant donné que les dispositions en question du Code criminel ont été rédigées à une époque où les ordinateurs n'existaient pas, leur formulation n'est pas adaptée aux nouvelles techniques. Pourtant, vu les progrès rapides de la technologie, l'ordinateur va sans doute jouer un rôle croissant dans nos vies quotidiennes. Il est manifestement nécessaire de prendre des mesures législatives pour tenir compte de cette nouvelle technologie et protéger la société de ses conséquences négatives. Vu l'attitude de l'ordinateur à traiter des volumes considérables d'informations précieuses à caractère commercial ou personnel, des mesures appropriées doivent être prises dès maintenant avant que quiconque ne subisse des pertes importantes d'argent ou de données à caractère personnel.

13. Les témoins qui ont comparu devant le Sous-comité sont convenus qu'il est nécessaire de prévoir des sanctions pénales pour combler les lacunes qu'a fait apparaître l'affaire McLaughlin. Néanmoins, on s'entend fort peu sur la forme de ces sanctions. Certains témoins sont d'avis que les sanctions pénales ne devraient constituer qu'une des solutions possibles et qu'il faudrait également améliorer les recours existants ou en créer de nouveaux. Cette opinion est partagée par les membres du Sous-comité. Selon nous, il est important d'examiner et d'appliquer tous les recours possibles lorsqu'ils sont appropriés, de façon à réserver les sanctions pénales aux cas extrêmes.

A. Le phénomène informatique

6. Depuis son avènement en 1946(2), l'ordinateur a pris une telle importance dans le traitement de toutes sortes d'informations qu'il est difficile d'imaginer une grande entreprise pouvant fonctionner sans lui. D'après l'industrie, près de 40 millions de dollars sont transférés chaque jour par des systèmes informatiques au Canada. Aux Etats-Unis, le chiffre atteint près de 400 millions de dollars. A l'échelle mondiale, il s'élève à 600 millions de dollars.(3)
7. Outil indispensable à l'entreprise et au secteur public, l'ordinateur s'introduit maintenant dans les foyers au moyen de consoles de la taille d'une machine à écrire pouvant être branchées sur un écran de télévision. Quiconque possède un compte en banque ou effectue des transactions de crédit utilise régulièrement les services d'un ordinateur. Un témoin a fort à propos donné l'exemple suivant:

«Aujourd'hui, depuis que j'ai quitté ma maison à Toronto, j'ai été au moins trois fois en contact avec un ordinateur. En début de matinée, j'ai pris l'avion pour Montréal et l'ordinateur d'Air Canada m'a émis ma carte d'embarquement. A midi, j'ai pris le train pour Ottawa et VIA Rail m'a émis un billet par ordinateur. Je me suis ensuite rendu à la Banque de Commerce, j'ai sorti ma carte VISA et j'ai fait un retrait de 100 dollars.»(4)

Bref, l'ordinateur est en train de s'intégrer à toutes les facettes de l'activité humaine. Il peut recueillir, stocker, mettre en corrélation, transférer et extraire des volumes de données considérables avec une facilité et une rapidité relatives. Son utilité actuelle est indéniable, mais les progrès technologiques futurs en feront un outil presque indispensable.

8. Il y a cependant un revers à toute médaille. A cause de l'aptitude de l'ordinateur à traiter de vastes quantités d'informations précieuses, certains y ont vite vu la possibilité tentante de l'utiliser de façon abusive. On a déjà entendu parler des «pirates de l'informatique» qui, avec une connaissance élémentaire du fonctionnement des ordinateurs, s'infiltrèrent dans des terminaux téléphoniques et des micro-ordinateurs personnels. Dans certaines universités, des «concours» sont organisés pour voir quel étudiant réussira le premier à déjouer les systèmes de sécurité d'un ordinateur, parfois même avec les encouragements du professeur. Des employés mécontents peuvent placer une «bombe logique»* dans le système informatique de dollars, en utilisant l'ordinateur pour virer des fractions de cents sur des comptes fictifs. Des employés mécontents peuvent placer une «bombe logique»* dans le système informatique, bombe à retardement qui «explosera» et détruira des programmes importants après que l'employé aura quitté l'entreprise.

9. Au Canada, deux cas de piratage en particulier ont fait la manchette. D'abord, dans l'affaire de l'école Dalton de 1980, un groupe d'élèves de huitième année d'une école privée de New York s'est servi du micro-ordinateur de l'école pour pénétrer dans les bases de données d'un certain nombre d'entreprises canadiennes et du gouvernement fédéral. Leur

* Une «bombe logique» est un programme, secrètement inséré dans le système informatique, qui permet d'endommager le logiciel ou le matériel dans des conditions déterminées à l'avance. Par exemple, un programmeur du service de la paye pourrait placer une «bombe logique» dans le système d'information sur le personnel: si son nom était un jour supprimé du fichier, ce qui signifierait qu'il a cessé de travailler pour l'entreprise en question, le programme secret serait automatiquement activé et toutes les données sur le personnel en mémoire seraient effacées.

comité est particulièrement redevable aux représentants du ministère de la Justice de leur collaboration et à Mme Susan Hubbell Nycum, du cabinet juridique californien *Gaston, Snow and Ely Bartlett*, d'avoir eu l'amabilité de nous faire part de ses constatations sur l'expérience américaine. Le Sous-comité tient également à remercier le greffier du Sous-comité, M. Pierre de Champlain, et Mme Monique Hébert, du Service de recherches de la Bibliothèque du Parlement, pour leur aide pendant les travaux et la préparation du rapport.

La présidente,
Céline Hervieux-Payette

5. Le Sous-comité est profondément reconnaissant à ces personnes qui ont généreusement donné de leur temps et accepté de nous faire profiter de leurs connaissances. Les nombreux points de vue différents présentés au Sous-Comité lui ont été extrêmement utiles et lui ont donné un tableau d'ensemble satisfaisant de bon nombre des questions visées. Le Sous-

4. Pendant les audiences, qui ont commencé le 17 mars 1983, le Sous-comité a entendu un grand nombre de témoins de professions variées.⁽¹⁾ Ont comparu des particuliers et des groupes spécialisés dans des domaines divers comme les techniques informatiques, la sécurité et la gestion, le droit de l'informatique, le droit de la propriété intellectuelle, l'application de la loi, les milieux bancaires, le droit en matière de protection des renseignements personnels et de protection des consommateurs.

3. Selon le Sous-comité, cette façon de procéder a donné des résultats très satisfaisants. Les travaux ont été efficaces et productifs grâce au petit nombre de membres du Sous-comité et à l'atmosphère non partisane qui a régné pendant les délibérations. Pour ces raisons, nous pensons que l'on devrait recourir plus souvent à de petits sous-comités pour l'étude des nombreuses questions qui intéressent le Parlement.

2. Déposé en première lecture par l'honorable Perrin Beatty le 16 décembre 1982, le projet de loi C-667 a été retiré de la deuxième lecture le 9 février 1983 et renvoyé au Comité permanent de la justice et des questions juridiques. Un sous-comité représentant les trois partis a été créé le 10 mars 1983. Le groupe de travail était en fait composé de la présidente, Me Céline Hervieux-Payette, député, de M. Kenneth Robinson, c.r., député, et de l'honorable Perrin Beatty, député.

1. Le Sous-comité a pour mandat d'examiner les questions visées par le projet de loi C-667, Loi modifiant le *Code criminel* et la *Loi sur la preuve au Canada* en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs.

INTRODUCTION

7. Le Sous-comité recommande que le gouvernement fédéral effectue une étude en profondeur sur la possibilité d'étendre aux programmes informatiques la protection visant les brevets et les dessins industriels (par. 56).
8. Le Sous-comité recommande aux gouvernements fédéral et provinciaux d'étudier à fond, conjointement, le droit relatif au secret industriel et d'adopter les mesures correctives qui s'imposent (par. 58).
9. Le Sous-comité recommande que l'industrie de l'informatique adopte ses propres règlements pour veiller à ce que ses membres aient une conduite irréprochable (par. 65).
10. Le Sous-comité recommande que les professeurs d'informatique soient tenus d'être qualifiés dans le domaine de l'éthique en informatique et que les responsabilités morales liées à l'utilisation d'ordinateurs figurent dans les cours d'informatique de tous les niveaux (par. 67).

RECOMMANDATIONS

1. Le Sous-comité recommande de modifier le *Code criminel* afin de créer deux nouvelles infractions: l'utilisation non autorisée d'un système informatique (sans apparence de droit) et la modification ou la destruction non autorisées (sans apparence de droit) de données informatisées. Le Sous-comité recommande en outre que les avocats de la Couronne aient le choix entre la déclaration sommaire de culpabilité et l'inculpation (par. 37).

2. Le Sous-comité recommande que les définitions nécessaires à la description des infractions portent le plus possible sur les fonctions exécutées et non sur les techniques en cause (par. 38).

3. Le Sous-comité recommande d'étudier à fond toutes les questions liées à la détection des délits informatiques et aux poursuites contre leurs auteurs, particulièrement en ce qui concerne l'étendue des pouvoirs de perquisition et de saisie, ainsi que les lois fédérales et les traités portant sur les enquêtes internationales et l'extradition; il y aurait lieu également d'étudier l'application, aux communications entre ordinateurs, des dispositions du *Code criminel* en matière d'écoute électronique (par. 47).

4. Le Sous-comité recommande de faire tous les efforts possibles pour veiller à ce que les policiers et les avocats de la Couronne qui pourraient être amenés à s'occuper de criminalité informatique reçoivent une formation leur permettant de s'acquitter efficacement de leurs fonctions (par. 48).

5. Le Sous-comité recommande que l'industrie de l'informatique et les organismes usagers évaluent les faiblesses de leurs systèmes et adoptent les mesures de sécurité nécessaires (par. 51).

6. Le Sous-comité recommande de modifier la *Loi sur le droit d'auteur* pour y inclure les logiciels informatiques (par. 55).

TABLE DES MATIÈRES

Page	
7	RECOMMANDATIONS
9	INTRODUCTION
11	A. Le phénomène informatique
13	B. Fréquence des délits informatiques.....
14	C. Le droit pénal : situation actuelle
15	D. Le droit pénal : modifications proposées
17	E. La Loi sur la preuve au Canada
18	F. Les problèmes d'application de la Loi
19	G. Mesures supplémentaires
19	1. Normes de sécurité
19	2. Recours au civil.....
21	3. Code d'éthique
23	CONCLUSION
23	DÉMANDE EN VERTU DU PARAGRAPHE (13) DE L'ARTICLE 69 DU RÈGLEMENT DE LA CHAMBRE DES COMMUNES.....
25	NOTES
27	ANNEXE «A»: LISTE DES TÉMOINS
29	ANNEXE «B»: BIBLIOGRAPHIE SOMMAIRE

Le Comité permanent de la justice et des questions juridiques a l'honneur de présenter son

NEUVIÈME RAPPORT

Conformément à son Ordre de renvoi du mercredi 9 février 1983, votre Comité a confié à un Sous-comité l'étude de l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs.

Le Sous-comité a présenté son rapport final au Comité. Votre Comité a adopté ce rapport avec modifications et demande que le gouvernement étudie l'opportunité d'appliquer les recommandations contenues dans le rapport.

Le rapport du Sous-comité, tel que modifié, se lit comme suit:

Publié en conformité de l'autorité du Président de la Chambre des communes
par l'imprimeur de la Reine pour le Canada
En vente: Centre d'édition du gouvernement du Canada, Approvisionnement et
Services Canada, Ottawa, Canada K1A 0S9

Published under authority of the Speaker of the House of Commons by the
Queen's Printer for Canada
Available from the Canadian Government Publishing Center, Supply and
Services Canada, Ottawa, Canada K1A 0S9

Tuesday, June 14, 1983
Thursday, June 16, 1983
Tuesday, June 21 1983

Chairman: Céline Hervieux-Payette

*Minutes of Proceedings and Evidence
of the Sub-committee on*

Computer Crime

Le mardi 14 juin 1983
Le jeudi 16 juin 1983
Le mardi 21 juin 1983

Président: Céline Hervieux-Payette

*Procès-verbaux et témoignages
du Sous-comité sur*

Les infractions relatives aux ordinateurs

*du Comité permanent de la justice et
des questions juridiques*

CONCERNANT:

RESPECTING:

Ordre de renvoi

Order of Reference

Y COMPRIS:

INCLUDING:

Rapport final

Final Report

Première session de la

rente-deuxième législature, 1980-1981-1982-1983

First Session of the

Thirty-second Parliament, 1980-81-82-83

SOUS-COMITÉ

SUR LES INFRACTIONS RELATIVES AUX ORDINATEURS

PRÉSIDENTE:

Mme Céline Hervieux-Payette, Lib., (Montréal-Mercier), Qué.
M. Ken Robinson, Lib., (Etobicoke-Lakeshore), Ontario
L'hon. Perrin Beatty, P.C., (Wellington-Dufferin-Simcoe) Ontario

PERSONNEL

Mme Monique Hébert, Services des recherches, Bibliothèque du Parlement
Pierre de Champlain
Greffier du Sous-comité

JUN 1983

COMITÉ PERMANENT
DE LA
JUSTICE ET DES QUESTIONS JURIDIQUES

RAPPORT DU SOUS-COMITÉ SUR LES INFRACTIONS RELATIVES AUX ORDINATEURS

CHAMBRE DES COMMUNES
CANADA





CANADA

INDEX

SUBCOMMITTEE ON

Computer Crime

OF STANDING COMMITTEE ON
JUSTICE AND LEGAL AFFAIRS

HOUSE OF COMMONS

Issues 1-18

•

1983

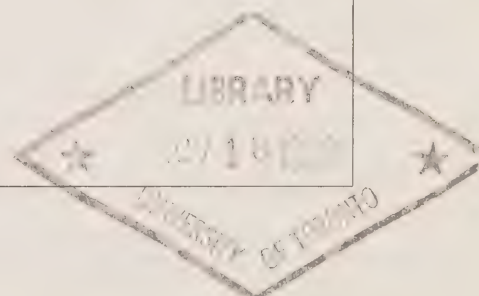
•

1st Session

•

32nd Parliament

Chairman: Mrs. Céline Hervieux-Payette



Published under authority of the Speaker of the House of Commons by the Queen's Printer for Canada

Available from Canadian Government Publishing Center, Supply and Services Canada, Hull, Québec, Canada K1A 0S9

INDEX

HOUSE OF COMMONS COMMITTEES—OFFICIAL REPORT

FIRST SESSION—THIRTY-SECOND PARLIAMENT

Abbreviations: A.=Appendices. Amdt.=amendment. M.=motion. S.O.=standing order.

DATES AND ISSUES

—1983—

March:	10th, 15th, 17th, 1; 23rd, 2.
April:	19th, 3; 27th, 4.
May:	3rd, 5; 10th, 6; 11th, 7; 17th, 8; 18th, 9; 19th, 10; 24th, 11; 25th, 12; 26th, 13; 31st, 14.
June:	1st, 15; 8th, 16; 9th, 17; 14th, 16th, 21st, 18.

Access to information, legislation, Que., 5:21, 27, 35; 14:23

Air traffic controllers, see Computers—Dependence

Alberta Institute of Technology, see Surveys and studies—Legislation

Allen, Superintendent George W. (Commercial Crime Branch, Royal Canadian Mounted Police)

Criminal Code Bill (computer crime—C-667) (subject matter), 1:32-40, 45-51

Appendices

Canadian Bar Association, 16A:1-16

Computers, 16A:8-9

Evidence Act, 1982, 13A:1-17

Privacy, 5A:1-12

United States, 15A:1-6

Art, see Copyrights—Computer-generated

Avison, Mr. Neville (Chief, Research and Statistics, Justice Department)

Criminal Code Bill (computer crime—C-667) (subject matter), 1:41, 48-9

Banks and banking

Automatic teller machines, abuse, 2:30, 35; 4:16-9; 13:13; 15:5, 14-6

Computer system, down-time, 13:13

Electronically transferred funds, interception, 6:7; 14:4-9; 15:16

Ontario Attorney General 1978 task force, 5:23

Impact, prevention, detection, etc., 4:4, 7, 14-6; 13:11

Offences, Professor Kittler, Apr. 25/83, *Globe and Mail* article, 13:5-6

Privacy, protection, need, 5:23-5, 32; 7:16; 8:17-20; 9:24; 13:15, 25; 14:6-8, 20-1; 15:16

Security systems, 13:5, 12, 17-25, 29; 14:10; 17:20, 24-5

See also Credit cards; West Germany

Beatty, Hon. Perrin (PC—Wellington-Dufferin-Simcoe)

Banks and banking, 5:23-5; 8:17-20; 9:24; 13:13-5; 14:20-1; 15:16; 17:24

Bell Canada, 6:28

Computer services, 2:12, 20, 30-1; 4:9-10, 23; 7:25-6; 8:9-11; 9:21, 25-8; 12:9; 13:11-4, 17, 28; 15:16-9; 16:13-5

Computers, 4:22; 6:12-4; 7:21; 16:13-7

Copyrights, 5:12-5; 7:20-3, 32; 8:10; 9:21-3; 13:14; 14:15; 16:18, 24-6, 34

Criminal Code, 2:22; 5:28; 7:25; 8:9-11; 15:18

Criminal Code Bill (computer crime—C-667) (subject matter),

1:13-8, 31-2; 2:4, 12-23, 30-5; 4:8-14, 19, 22-6; 5:5-7, 12-7,

21-30, 36; 6:8-23, 27-8, 31; 7:19-27; 8:4, 7-20; 9:13, 17, 21-8;

12:9-12, 13:7-20, 28-9; 14:15-21, 24; 15:4, 12-21; 16:13-28, 34;

17:11, 21-8

Data, 2:22; 4:11-2; 5:16-7, 29; 7:21-6, 31-2; 8:11; 9:26; 12:9-10;

13:14-6, 19; 15:17-8; 16:25-7; 17:23

Data theft and/or destruction, 4:24-6; 5:17, 25; 6:9-10, 14-7, 20-1; 7:19; 16:18-24

Evidence, 17:22-7

Evidence Act, 1982, 13:7-8; 17:23-5

Government, 2:18-9; 6:31

Gun control legislation, 12:10

House of Commons, 6:10

Industry, 13:13-4, 19-20

Investigation and enforcement, 4:22; 5:16, 28; 7:26-7; 13:9-10; 15:13-5

Jurisdiction, 2:16; 4:22-3; 5:24; 7:20-3; 9:22, 28; 15:17-8; 16:19-21, 24

Legislation, 4:24

Medical records, 14:24

Beatty, Hon. Perrin—Cont.

Offences, 2:16, 21; 4:9-13; 5:28-9; 6:16; 7:21-6; 8:10-1; 9:23-6; 12:9-12; 13:10-1, 14-7; 15:13-4; 16:17, 22-5, 28

Official Secrets Act, 17:23-4

Organization meeting, 1:8-13

Points of order

Chairman, 8:4

Documents, 1:13, 32; 6:8

Ms., 5:4; 13:7-10

Meetings, 1:10-1, 14-5

Members, 1:12

Printing, M., 18:30

Questioning of witnesses, 1:32; 2:4

Witnesses, 1:14-5, 32; 4:24

M., 15:4

Prevention/deterrence, 2:31, 35; 4:8, 23; 6:13-7; 7:19; 8:12-3;

12:10-2; 13:13-4; 14:18

Privacy, 5:26-30; 7:26; 8:16-20; 9:24; 13:15; 14:15-21

Privacy Act, 14:19

Security, 2:17-20; 7:26, 32; 8:7-8, 13-6; 12:10-2; 13:11, 14-20, 28; 15:20; 16:25

Social insurance number, 17:26-7

Subcommittee, 1:17-8

Surveys and studies, 2:16; 9:22-3; 15:13-4

Sweden, 7:21; 9:25

Television, 6:11, 16-7, 27-8; 8:12

United States, 4:22; 5:28; 15:15-8

Universities, 5:25; 13:15; 14:18

Wiretapping and eavesdropping, 6:10-2, 17

Bell Canada, telephone extensions, detection, 6:28

Bills, see titles of particular bills

C-667. Criminal Code amdt. (computer crime) (subject matter).

Mr. Beatty

Bisanz, Ms. Christine (Acting Director of Association and Activities, Consumers' Association of Canada)

Criminal Code Bill (computer crime—C-667) (subject matter), 14:23-4

Blanchard, Mr. Bernard E. (Executive Director, Canadian Bar Association)

Criminal Code Bill (computer crime—C-667) (subject matter), 16:30, 33-5

Boire, Mr. Paul C. Sr. (President, Canadian Association of Data Processing Service Organizations (CADAPSO))

Criminal Code Bill (computer crime—C-667) (subject matter), 10:5-14, 17-25

Britain

Music, copyright law, 7:7; 11:6

Privacy, data protection, legislation, 5:20

Brookings Institution, see Symposium on Computer Crime and Privacy

Butler, Mr. Tony (Senior Policy Advisor, Consumer and Corporate Affairs Department)

Criminal Code Bill (computer crime—C-667) (subject matter), 11:6-22

CA magazine, see Offences—Watkins

CBEMA, see Canadian Business Equipment Manufacturers Association

CIPS, see Canadian Information Processing Society

Canada Evidence Act, see Evidence Act, 1982

Canadian Association of Data and Professional Service Organizations (CADAPSO)

Role, objectives, 10:6-7, 19-20

Task force submissions, 10:11-4

See also Organizations/individuals appearing and briefs submitted

Canadian Bankers' Association, *see* Evidence Act, 1982;

Organizations/individuals appearing and briefs submitted

Canadian Bar Association

Draft legislation, future submissions, etc., 16:4-5, 15-8, 25, 30-5, 40-1; 16A:1-16; 17:11-2

See also Organizations/individuals appearing and briefs submitted

Canadian Business Equipment Manufacturers Association (CBEMA)

Discussion Paper on Computer Abuse, 3:12, 15

Role, 3:5

See also Organizations/individuals appearing and briefs submitted

Canadian Information Processing Society (CIPS)

Role, operations, 12:4-5, 11-8

See also Organizations/individuals appearing and briefs submitted

Carroll, John, *see* Surveys and studies—Employee attitudes

Cerberus Computer Security Inc., *see* Organizations/individuals appearing and briefs submitted

Chairman and Vice Chairman, decisions and statements, *see*

Procedure and decisions of the Chair

Charter of Rights and Freedoms, *see* Privacy

Child abuse, reporting requirement, 16:38

Chrétien, Hon. Jean, *see* Criminal law

Communications, *see* Computers

Computer Crime Project, Justice Department

Mandate, consultations, etc., 1:20-31, 41, 44, 48; 9:4-5

Proposal, Criminal Code, amending, 1:20, 50

Computer services, unauthorized use, 1:21-2, 33-4, 46-7; 3:10-1, 31;

4:10; 7:5, 9-10; 8:10-1; 9:7, 10, 25-30; 11:5-7, 19-20; 13:9-13, 16; 15:6, 18, 27; 16:6; 17:5, 14

Government systems, 1:49

Industrial espionage, 1:34, 47; 9:26; 12:9

Publications, encouraging, *TAP*, etc., 2:9; 8:9-10

Sabotage, system crashes, etc., 1:34-5; 2:17; 3:8, 22; 13:9-13, 17; 15:6-7, 16

"System hacking", 1:34; 2:7, 13, 17-9, 26; 3:8, 22, 25; 4:4, 8-10, 23; 7:4, 7, 15; 8:21; 9:9, 13; 10:18; 13:9-13, 28-9; 15:9, 24

Dalton School, N.Y., 2:7, 12-3, 18-20, 30; 4:23; 7:6-7, 13, 18, 31; 9:22; 13:14

University of Waterloo, 7:4, 7; 13:28-9

Theft of computer time, 7:15; 13:11-2; 16:6, 14-5

Time-sharing systems, 2:31-2; 3:7-8; 4:9-10; 7:25-6; 15:19; 16:14-5

University of Alberta, McLaughlan case, Supreme Court decision, 1:19, 44; 2:8; 3:10-1; 5:25; 7:10-1, 29; 9:21; 16:5-6, 13-4; 17:6

Computers

Communications

Capabilities, electronic mail, etc., 7:9-13, 29-30; 14:7

System, packet switching, 1:35; 4:22-3; 6:12-3

See also Investigation and enforcement

Costs, decrease, 6:12-4; 7:9; 12:12

Defining, 3:12-6; 4:20; 7:5-7, 12, 21, 24; 10:21; 16:6-7, 11-2, 15-7, 31, 35; 16A:8-9; 17:6, 11

Dependence, hospitals, air traffic controllers, etc., 2:21, 29; 4:12; 16:17

Errors, monetary losses, 15:10, 25-6

Computers—*Cont.*

Proliferation, 2:15, 18-9; 7:12, 15; 10:21; 16:27

Technology, impact on society, 1:20, 23, 28; 3:5-7; 4:18; 7:29; 14:4-5

Constitution, *see* Charter of Rights and Freedoms

Consumer and Corporate Affairs Department, *see*

Organizations/individuals appearing and briefs submitted; Surveys and studies

Consumers' Association of Canada

Role, 14:4

See also Organizations/individuals appearing and briefs submitted; Privacy

Conway, Mr. Dave M. (Manager, Resources Protection, Mitel Corporation)

Criminal Code Bill (computer crime—C-667) (subject matter), 8:6-22

Copyrights

Computer chip design, 5:15; 7:32

Computer-generated art and music; 5:14-5

Criminal sanctions, revising, 1:28; 11:17

International treaties, 9:23; 11:12-6, 20

Legislation, review, 4:21; 5:12; 9:8; 10:12; 11:5-6, 16-7, 21; 16:29, 34

Lifespan, 11:6-7, 15, 20-2

Software protection, 3:26-7; 4:21-2; 5:6-14, 17; 7:7-9, 20-3; 8:10; 9:19-23; 10:10-2; 11:5, 11-9; 12:20; 13:14-5, 26; 14:15; 15:25; 16:18, 24-8; 17:14

Video games, protection, 5:13; 9:9-10; 11:6

See also Britain; Data—Protection; Japan

Couchman, Mr. Bruce (Policy Advisor, Consumer and Corporate Affairs Department)

Criminal Code Bill (computer crime—C-667) (subject matter), 11:4-6, 11-21

Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *see* Privacy—Data protection

Credit cards, offences, 13:10-2; 16:9

Criminal Code

Amending, 1:39, 43; 3:21, 28; 4:20; 5:10; 6:32; 7:28-9; 8:9-11, 14, 23; 9:8, 22, 25-30; 10:15-6; 11:18; 12:20, 23; 13:26; 15:18; 16:30, 36

Conduct of crime/technology, emphasizing, 1:21-2; 2:9-10, 22-3, 37-8; 3:11; 4:8-9; 5:28; 7:13, 25; 12:8; 17:4

Justice Department, theft and fraud project, 1:19, 22

Offences, summary conviction and indictment, 16:38

See also Computer Crime Project; Data theft and/or destruction; Investigation and enforcement—Offences—Search; Law Reform Commission; Offences—Identifying

Criminal Code Bill (computer crime)—C-667 (subject matter). Mr. Beatty

Consideration, 1:13-52; 2:4-38; 3:5-31; 4:4-26; 5:3-37; 6:4-32; 7:4-34; 8:4-24; 9:4-36; 10:5-26; 11:4-22; 12:4-25; 13:4-30; 14:4-24; 15:4-33; 16:4-41; 17:4-34

Definitions, 16:5-12, 15-24, 32-3; 17:6-9

Criminal law, review, Justice Department, former Minister Jean Chrétien, 1:19; 16:30

DES, *see* Data encryption standard

Dalton School, N.Y., *see* Computer services

Data

Post-industrial society, role, 9:5-6

Data—Cont.**Proprietary treatment**

Conceptual difficulties, MacBain comments, etc., 1:24, 44; 2:22; 9:10

Defining, 6:23-5; 11:4-6, 19; 13:16, 20-2; 14:9, 12-3; 16:7-9, 26; 17:12

Legislation, amending, 1:23-5, 28; 3:9; 5:5-7, 11; 8:11; 10:14-6, 24; 11:10, 18-20; 12:8-9; 14:10-2; 17:7-9

Valuation, 1:38-40; 3:8, 11; 4:11-2; 5:12, 29; 7:15, 21-4; 12:11; 17:6

Protection

Copyrights, trademarks, patents, etc., 1:24-8, 39, 43; 3:6-9; 4:21; 5:16-7; 7:31-2; 9:7, 17-9, 22-5, 34-5; 10:16; 11:4-19; 12:9

Industrial Design Act, 11:16-8

Manual/computer-stored, 7:21, 26; 8:11; 9:26; 12:10; 13:6; 15:17-8; 16:25-7, 36; 17:18

Trade secret law, 9:8, 15-7, 26-8, 30-1, 34-5; 10:10; 11:9, 17-8; 12:9; 13:14-5, 26; 15:17-21; 16:25; 17:23

Storage, back-up systems, 2:18; 3:24-5; 4:11, 16; 7:8; 13:18-9

Eaton's of Canada Limited, 1950 system crash, 2:18

Revenue Department, taxation data, 2:19-20

Vs information, defining, 10:13; 16:7; 17:8, 12-3, 30

See also Government; Privacy; Sweden

Data encryption standard (DES), see Security

Data theft and/or destruction, 1:21-3; 2:32-3; 3:6-8, 13, 26-7; 4:8-11; 5:17; 6:15-6; 9:7; 13:9, 27; 16:23-4

Criminal Code, amending, 1:39; 9:10; 14:8-13, 22; 16:8-11, 18-21, 36

Detection, 2:32-3; 3:6; 5:7-10; 7:6-7, 10, 16, 19; 14:7

"Diddling", altering data, 15:7-8

"Diversion" of data, 16:8-9, 18-21

Electro-magnetic pulse (EMP), effect, 6:8-9, 15, 20-1; 9:34

Microcomputer software, appropriation, 5:6-10; 9:11, 17

Remote access, electro-magnetic radiation (EMR), tempestization, etc., 6:4-10, 14-21, 24, 28-30

Software "time bombs", 4:24-6; 7:16-7; 16:10, 21-2

Telephone access, 7:17-8, 22; 14:7

Trojan horse scheme, access code theft, 7:17

Datacrown Inc., see Organizations/individuals appearing and briefs submitted

Dean, Mr. John (Senior Legal Advisor, IBM, Canadian Business Equipment Manufacturers Association, Toronto (CBEMA))
Criminal Code Bill (computer crime—C-667) (subject matter), 3:8-9, 13-8, 23-31

Definition, 4:17; 6:15; 15:5, 14, 21-3, 26; 16:32-3

See also Criminal Code Bill

Deterrence, see Prevention

EMP, see Electro-magnetic pulse

EMR, see Electro-magnetic radiation

Eaton's of Canada Limited, see Data—Storage

Electro-magnetic pulse (EMP), see Data theft and/or destruction

Electro-magnetic radiation (EMR), see Data theft and/or destruction—Remote access; Television

Electronic mail, see Computers—Communications

Elliott, Ms. Christine (Member, Ontario Branch, Consumers' Association of Canada)
Criminal Code Bill (computer crime—C-667) (subject matter), 14:4-24

Encryption, see Security

Equity Funding Insurance, see Offences

Ethics, see Prevention/deterrence; Universities

Evidence

Admissibility, legislation amending, 1:26, 36-40; 5:8; 7:8, 16:11; 17:9-11, 15-22, 25, 28-33

McMullen case, Ontario Court of Appeal decision, 17:18-22

R. vs Bell and Bruce, decision, 17:22-3

Reliability, 17:15-6, 25-8, 31-2

Evidence Act, 1982 (Bill S-33), Uniform Law Conference recommendations, etc., 13:7-8; 13A:1-17; 16:34; 17:17-33
Canadian Bankers' Association position, 17:20, 23-5

Extradition treaties, see Investigation and enforcement

Federal-provincial relations, see Legislation

Finch, Mr. James H. (Cerberus Computer Security Inc., Toronto)
Criminal Code Bill (computer crime—C-667) (subject matter), 2:4-10, 18-22, 25-35, 38

Firmware, 16:7, 18

Fisk, Mr. George E. (Barrister, Gowling and Henderson Barristers)
Criminal Code Bill (computer crime—C-667) (subject matter), 9:11-25, 33-5

Flaherty, Mr. David H. (Professor, University of Western Ontario)
Criminal Code Bill (computer crime—C-667) (subject matter), 5:18-36

Fortier, Mr. Yves (President, Canadian Bar Association)
Criminal Code Bill (computer crime—C-667) (subject matter), 16:4-5, 13, 23, 29-34, 37-40

France, privacy, data protection legislation, 5:29-30

Fraud, see Offences—Defining—Equity Funding Insurance

Freedom of information legislation, impact, 1:27

Gaston, Snow and Ely Bartlett, see Organizations/individuals appearing and briefs submitted

Gentleman, Mr. Morvin (National Research Council)
Criminal Code Bill (computer crime—C-667) (subject matter), 7:4-12, 19-23, 27-34

Georgas, Mr. Stephen (Solicitor, Toronto)
Criminal Code Bill (computer crime—C-667) (subject matter), 17:4-16

Globe and Mail, see Banks and banking—Offences

Government

Data banks, security, 1:49; 2:7, 18-9; 4:7; 6:29-31; 9:7; 13:20

See also Computer services; Privacy—Data protection; Security

Gowling and Henderson Barristers, see Organizations/individuals appearing and briefs submitted

Gun control legislation, 12:10-1

Hammond, Mr. Grant (Professor, Counsel, Law Center, University of Alberta)
Criminal Code Bill (computer crime—C-667) (subject matter), 9:4-11, 25-33

References, see Surveys and studies—Legislation

Hardware

Protection, patent law, 11:7-8

Hardware—Cont.

Theft and/or destruction, 1:21-2, 33, 37
See also Offences

Henderson, Mr. J. Ian (Vice President and General Counsel, Landspan International of Canada Ltd.)

Criminal Code Bill (computer crime—C-667) (subject matter), 6:4, 7-17, 22-31

Hervieux-Payette, Mrs. Céline (L—Montreal-Mercier; Parliamentary Secretary to Solicitor General; Chairman)

Access to information, 14:23
 Canadian Bar Association, 16:33-4, 40-1
 Computer Crime Project, 1:48-50
 Computer services, 3:31; 8:21
 Computers, 7:29
 Copyrights, 3:26-7; 4:21-2; 11:11-2, 21
 Criminal Code, 3:28
 Criminal Code Bill (computer crime—C-667) (subject matter), 1:13-8, 31-2, 48-52; 2:4; 3:5-7, 21-31; 4:4, 20-2, 26; 5:5; 7:4, 12, 34; 8:20-4; 9:4, 35-6; 10:5, 14; 11:4, 7-8, 11-2, 21-2; 14:4, 23-4; 15:4, 32-3; 16:4, 11, 33-5, 40-1; 17:4, 16-7, 33-4
 Data, 11:11; 17:12-3
 Data theft and/or destruction, 3:26-7
 Election as Chairman, 1:7
 Evidence, 3:21
 Government, 1:49
 Hardware, 11:7-8
 Information, 4:21
 Jurisdiction, 3:23-4, 27; 15:32
 Medical records, 14:23-4
 Offences, 1:48-9; 8:22
 Organization meeting, 1:7-13
 Patents, 11:21
 Prevention/deterrence, 8:23
 Security, 8:21
 United States, 3:23; 15:32

Hill, Mr. Norman (Project Chief, Theft and Fraud Project, Justice Department)

Criminal Code Bill (computer crime—C-667) (subject matter), 1:18-32, 40-4, 48-51; 17:24-5, 33-4

Hnatyshyn, Hon. Ray (PC—Saskatoon West)

Organization meeting, 1:7-11
 Point of order, meetings, 1:10

Hospitals, see Computers—Dependence**Hotel industry, see** Industry**House of Commons, security, 2:33**

Local area network, 6:10

Human rights legislation, see Security—Employee screening**IBM Corporation, see** Security**Income tax, see** Data—Storage; Television—Electro-magnetic radiation**Industrial Design Act**

Revision, 11:21
See also Data—Protection

Industry

Concern, 10:5, 19; 12:5-6, 17, 24
 Impact, 2:6-8, 15-7; 3:6; 12:6; 13:13-4
 Hotel reservation systems, 2:17; 13:19-20
See also Computer services; Prevention/deterrence;
 Security—Corporate responsibility

Information, see Data—Vs**Institute of Internal Auditors Inc., see** Surveys and studies—Employee attitudes**Insurance, see** Equity Funding Insurance; Security**Intellectual/industrial property, definitions, 11:20-1****Interdepartmental committee, 1:28****Investigation and enforcement**

Computer communications, lawfully intercepting, legislative amendment, 1:35, 38, 45-6
 Costs, 5:16
 Extradition treaties, applying, 1:26-7, 39-40
 Reporting rates and requirements, 1:22-3; 2:16; 3:6, 22, 28; 4:5-6, 22; 5:9, 28; 7:18, 26-7; 12:8, 19-21; 13:7, 10, 26-9; 14:10; 15:13-5; 16:37-40
See also Child abuse; United States
 Search and seizure, Criminal Code, amending, 1:26, 36-40

J. Walter Thompson Co., see Offences**Japan, software, copyright protection, 10:19; 11:13****Jestin, Mr. E.** (Supervisor, Internal Control, Evaluation, The Bank of Nova Scotia, Canadian Bankers' Association)

Criminal Code Bill (computer crime—C-667) (subject matter), 13:13, 17-9, 22-9

Juliani, Mr. Tony J. (Professor, Department of Criminology, University of Ottawa)

Criminal Code Bill (computer crime—C-667) (subject matter), 8:4-10, 13-9, 22-3

Jurisdiction

Civil/criminal, 1:41-3; 2:7-9, 16, 29; 3:11, 19, 23, 27; 4:21-2; 5:6-7, 10-2, 24, 33; 6:32; 7:20-3; 9:7-10, 14-5, 22, 26-33; 10:15-6, 25; 11:9, 17; 13:20-1, 27; 15:17-8, 22-8, 31-2; 16:24-5, 28; 17:13
 International arena, 1:26, 39; 3:24; 4:22-3; 9:22; 10:24-5; 16:18-21

Justice Department, see Computer Crime Project; Criminal Code; Criminal law; Organizations/individuals appearing and briefs submitted**Kaufman, Mr. Howard** (Vice President, Xerox, Canadian Business Equipment Manufacturers Association, Toronto (CBEMA))

Criminal Code Bill (computer crime—C-667) (subject matter), 3:9-30

Kay, Mr. D.W. (District Manager, Datacrown Inc.)

Criminal Code Bill (computer crime—C-667) (subject matter), 10:14-8, 25

Kingston, Ms. Judith (Standing Committee on Law, Science and Technology, Canadian Bar Association)

Criminal Code Bill (computer crime—C-667) (subject matter), 16:5-15, 18-24, 27-9, 33-4, 37-40

Kittler, Anne, see Banks and banking—Offences**Krever Commission, see** Medical records**Lachance, Mr. Claude-André** (L—Rosemont; Parliamentary Secretary to Minister of State for Trade)

Organization meeting, 1:7-12
 Points of order
 Documents, 1:12
 Election of Chairman, M., 1:7
 Election of Vice Chairman, 1:7-8
 Meetings, 1:10-1
 M., 1:11

Lachance, Mr. Claude-André—Cont.

Points of order—*Cont.*

Members, 1:12

Printing, M., 1:8

Quorum, 1:12

M., 1:8

Witnesses, 1:11

Ms., 1:9

Subcommittee, 1:10

M., 1:8

Landspan International of Canada Ltd.

Role, 6:4, 29

See also Organizations/individuals appearing and briefs submitted

Laser beams, *see* Wiretapping and eavesdropping

Law Reform Commission, Criminal Code review, 1:50-1; 16:30

Lawrence, Mr. Peter J. (President/Director, Landspan International of Canada Ltd.)

Criminal Code Bill (computer crime—C-667) (subject matter), 6:4-32

Learnmouth, Ms. Pat (Co-ordinator of Communications, Canadian Bankers' Association)

Criminal Code Bill (computer crime—C-667) (subject matter), 13:9-10, 15-7, 20-2, 26-7.

Legislation

Federal/provincial, discussions, etc., 1:25-6, 39, 43-4; 4:19; 5:35-6; 9:9, 29-30, 33

International perspective, 4:24; 15:12, 30-1; 17:17

See also Copyrights; Criminal Code; Data—Proprietary treatment; Evidence—Admissibility; Evidence Act, 1982; France; Freedom of information; Gun control legislation; Industrial Design Act; Investigation and enforcement—Computer communications; Manitoba; Patents; Prevention/deterrence; Privacy—Data protection, Standards—Personnel; Privacy Act; Property; Royal Canadian Mounted Police; Security—Employee—National—Standards; Surveys and studies; Trademarks; United States; West Germany

Local area networks, *see* House of Commons

MacBain, Al, *see* Data—Proprietary treatment

MacIntosh, Mr. Charles W., Q.C. (Standing Committee on Law, Science and Technology, Canadian Bar Association)

Criminal Code Bill (computer crime—C-667) (subject matter), 16:11, 16-22, 25-7, 31-2, 35-6, 40

MacIntosh, Mr. R.M. (President, Canadian Bankers' Association)

Criminal Code Bill (computer crime—C-667) (subject matter), 13:4-29

Manitoba, privacy legislation, 14:12

McLaughlan case, *see* Computer services—University of Alberta

McMullen case, *see* Evidence—Admissibility

Media, *see* Offences

Medical Records, confidentiality, Krever Commission, etc., 5:19, 32; 14:23-4; 17:24

Microcomputers, *see* Data theft and/or destruction

Microwaves, *see* Wiretapping and eavesdropping

Mischief, *see* Offences—Defining

Mitel Corporation (Kanata, Ont.)

Resources protection program, 8:6-8, 21

See also Organizations/individuals appearing and briefs submitted

Music *see* Britain; Copyrights—Computer-generated

NSA, *see* National Security Agency

National Research Council, *see* Organizations/individuals appearing and briefs submitted

National Security Agency (NSA), *see* Security—Tempestization

Newspapers, *see* *Globe and Mail*

Northern Alberta Institute of Technology, *see* Television—Pay TV

Nycum, Mrs. Susan H. (Attorney-at-Law, Gaston, Snow and Ely Bartlett, Palo Alto, California)

Criminal Code Bill (computer crime—C-667) (subject matter), 15:4-33

References, *see* United States—House of Representatives

OECD, *see* Organization for Economic Co-operation and Development

Offences

Canadian data, availability, 1:21; 4:6-7; 12:17; 13:10-1

Defining

Break and enter, 12:10, 24

Consensual criteria, 3:9-10; 4:9; 8:10

Criminal intent, 6:24-5, 31

Fraud, 7:15; 13:11-3; 15:5-6, 10-1, 16-7; 17:4-5, 8

Mischief, 9:25; 10:25; 11:19; 13:9, 14, 21; 16:9-12, 17, 23, 30, 36-7; 17:4-5

Physical damage, 16:17-8, 22-4

Possession of interception equipment, 6:25-6

Trespass, 4:9-10, 13-4, 19-20; 5:28-9; 6:16; 7:21-6; 8:10-2; 9:23-6; 11:6-7, 10; 12:9-10, 23-4; 13:14-7; 15:18-20; 16:24-5, 28

Employee abuse, 9:31, 34; 12:6-7, 12; 13:11-2; 15:8; 16:40

Equity Funding Insurance, fraud, 15:8

Hardware, destruction, exclusion, 13:9

Identifying in Criminal Code, 1:36-9; 7:14-5; 10:15, 24-5; 12:8

J. Walter Thompson Co., profits overstatements, 15:8

Monetary losses, 2:9, 14-5; 4:5-6, 12-3; 8:22

Occurrence, 1:32, 48-9; 2:16, 21-2; 4:6-7; 6:30; 10:5; 12:22; 13:4-6, 10-1, 20; 15:5, 13-4

Media, distorting, 13:4-6; 16:5

Public perception, 8:22; 12:18; 13:9; 15:9, 25

Victim, identifying, 6:24

Watkins, Peter, *CA* magazine, January 1981 article, *Computer Crime, Myth from the Reality*, 1:23; 2:16, 21-2; 4:6

See also Banks and banking; Computer services; Criminal Code; Data theft and/or destruction; Telecommunications

Offenders

Profile, 15:10-2

Restitution, 1:27; 3:20; 7:33

See also United States

Official Secrets Act, 17:23-4

Oil industry, seismic computerized information, effect, 9:4

Ontario, *see* Property

Ontario Attorney General, *see* Banks and banking—Electronically transferred funds

Ontario Court of Appeal, *see* Evidence—Admissibility

Ontario Lawyers' Weekly, *see* Software—Protection

Ontario Provincial Police, *see* Surveys and studies

Order of reference, Criminal Code Bill (computer crime—C-667) (subject matter), 1:3

Organization for Economic Co-operation and Development (OECD), *see* Privacy—Data protection

Organizations/individuals appearing and briefs submitted

Canadian Association of Data Processing Service Organizations (CADAPSO), 10:5-14, 17-25
 Canadian Bankers' Association, 13:4-29
 Canadian Bar Association, 16:4-40
 Canadian Business Equipment Manufacturers Association, Toronto (CBEMA), 3:5-31
 Canadian Information Processing Society (CIPS), 12:4-24
 Cerberus Computer Security Inc., 2:4-38
 Consumer and Corporate Affairs Department, 11:4-22
 Consumers' Association of Canada, 14:4-24
 Datacrown Inc., 10:14-8, 25
 Flaherty, Mr. David H., 5:18-36; 5A:1-12
 Gaston, Snow and Ely Bartlett, 15:4-33
 Georgas, Mr. Stephen, 17:4-16
 Gowling and Henderson Barristers, 9:11-25, 33-5
 Hammond, Mr. Grant, 9:4-11, 25-33
 Juliani, Mr. Tony J., 8:4-10, 13-9, 22-3
 Justice Department, 1:18-32, 40-4, 48-51; 17:17-34
 Landspan International of Canada Ltd., 6:4-32
 Mitel Corporation, 8:6-22
 National Research Council, 7:4-12, 19-23, 27-34
 Palmer, Mr. John, 5:5-17
 Peat, Marwick and Partners, 4:4-26
 Royal Canadian Mounted Police, 1:32-40, 45-51
 Spitzer, Mr. Frank, 7:12-9, 20-34

Packet switching, *see* Computers—Communications

Palmer, Mr. John (Professor, University of Western Ontario)
 Criminal Code Bill (computer crime—C-667) (subject matter), 5:5-17
 References, *see* Surveys and studies—Consumer and Corporate Affairs Department

Parker, Donn, *see* Surveys and studies; United States—House of Representatives

Patents

Canadians obtaining in U.S., 11:9-10
 Legislation, revision, 11:16, 21; 16:31
See also Data—Protection; Hardware

Pay TV, *see* Television

Peat, Marwick and Partners, *see* Organizations/individuals appearing and briefs submitted

Penalties, *see* Prevention/deterrence

Pitney Bowes Corporation, *see* White collar crime

Prevention/deterrence

Apprehension, prosecution, probability, 2:27, 35-6; 3:6, 16, 21-3; 5:6-10; 7:10, 13, 18-9; 8:5, 13; 10:15; 14:7, 14
 Cost/time prohibitive security measures, establishing, 6:13-4
 Industrial and ethical standards, development, 1:39; 2:27-31; 7:15; 9:32-3; 10:6-7, 10, 20; 12:10-2, 15-6; 13:25-6; 14:14-5, 18; 15:28-9; 16:39-40
 Legislation, 2:6, 10-1, 24-8, 34; 3:6; 4:8; 6:15-7; 7:34; 8:9-13, 23; 12:8-9; 13:13-4
 Penalties, 2:15, 27-8, 31; 3:11, 19-20, 28; 5:10; 9:15, 35; 12:23; 15:20, 30; 16:12
 Public awareness, expanding, 1:39; 2:24, 34; 4:23; 7:16-7; 12:6-7, 11-2; 14:8-9; 15:31

Prevention/deterrence—Cont.

Security measures, applying properly, 1:32-3, 45; 2:19, 27; 3:16, 19, 26; 4:14-5; 8:15; 12:9, 17; 14:13-4
See also Banks and banking—Impact; Security; White collar crime

Privacy

Charter of Rights and Freedoms, entrenching, 14:9-11, 18-20
 Consumers' Association of Canada, actions, advocacy, 14:8-9
 Data, de-personalizing, 5:25-7
 Data protection, 5A:1-12; 7:15-6, 26; 9:7; 10:10; 17:5, 12-3
 Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 5:22
 Government departments, contractors, 5:34; 9:24-5
 Individual responsibility, 14:8, 20-2
 International regulations, 5:20, 29-31
 Organization for Economic Co-operation and Development guidelines, 5:20-2, 27, 35
 Standards, developing, legislating, 5:18-21, 27-33; 8:16-20; 9:24; 14:5-23
 Defining, 14:19-20
 Personnel records, prevention of access, legislation, 5:25-6; 8:16
 Social insurance number, use, guidelines, 14:8, 18
See also Access to information; Banks and banking; Britain; France; Manitoba; Medical records; United States; West Germany; Wiretapping and eavesdropping

Privacy Act, 1:27, 39; 5:27, 32-4; 14:11, 19

Procedure and decisions of the Chair

Chairman, leaving meeting early, 2:4; 10:14
 Clerk, information, requesting, 1:44
 Clerk, participation, 1:7
 Documents
 Appending to minutes and evidence
 Ms. (Mr. Beatty), 5:4, agreed to; 13:7-10, agreed to, 3
 Ms. (Mr. K. Robinson), 15:33, agreed to, 3; 16:28, agreed to, 3
 Availability to members, 1:12-3
 Briefs
 Availability in both official languages, 1:20; 16:40; 17:33
 Distribution, 3:6; 6:8
 Studying, 1:32
 Submitted to Clerk, 1:24, 41
 Tabling, 1:20-2, 51; 13:7
 Election of Chairman, M. (Mr. Lachance), 1:7, agreed to, 4
 Election of Vice Chairman, unofficially, 1:7-8
In camera meetings, 18:29-30
 Meetings
 Adjourning, division bells ringing, 10:26
 Delays in starting, 6:4
 Extending hours, 2:31
 Scheduling, 1:10-1, 14-5, 52; 2:38; 9:36; 10:26; 16:41
 M. (Mr. Lachance), 1:11, agreed to, 4
 Members, alternates, 1:12
 Order of reference, clarifying, 1:8-9
 Printing, minutes and evidence
 Additional copies, M. (Mr. Beatty), 18:30, agreed to
 M. (Mr. Lachance), 1:8, agreed to, 4
 Questioning of witnesses
 Acting Chairman, rights, 2:4
 Chairman, participating, 3:21
 Insufficient time, re-calling, 1:31-2, 47
 Order, 1:40
 Quorum, meeting and printing evidence without
 M. (Mr. Lachance), 1:8, agreed to, 4
 Providing at least 2 members present, 1:12
 Reports to Committee, first, M. (Mr. K. Robinson), 2:4, agreed to, 3; second, 10:3, agreed to; final, M. (Mr. K. Robinson), 18:30, agreed to

Procedure and decisions of the Chair—Cont.

Reports to House, tabling, 16:33-5

Witnesses

Appearance before Committee, 1:25, 44, 48; 4:20

M. (Mr. Lachance), 1:9, agreed to, 4

Demonstration, providing, 1:48-9; 7:5

In camera, 2:6, 11-2, 38

Departmental officials, requesting, 1:14, 18

Expenses, Subcommittee paying

M. (Mr. Beatty), 15:4, agreed to, 3

M. (Mr. Lachance), 1:9-10, agreed to, 4

Information, requesting, 1:41, 48, 52; 3:31; 4:20, 24-6; 9:28; 12:16, 24-5; 15:31

List, 1:11, 14-6

Scheduling, 1:13-7

Statements

Distribution, 2:5

In advance, 13:4

Hearing, postponing questioning, 1:31-2

Length, 1:32

Reading, 5:18

Substitution, 16:41

Project Mac, see Security**Property**, ownership records, computerization, Ont. legislation, 14:5-6**Prosecution, see Prevention/deterrence—Apprehension; White collar crime****Quebec, see Access to information****Reid, Mr. John** (Chairman, Legislation Committee, Canadian

Business Equipment Manufacturers Association, Toronto

(CBEMA))

Criminal Code Bill (computer crime—C-667) (subject matter), 3:5-7, 11-2, 19-26, 29-31

Reports to Committee, first, 3:3; second, 10:3; final, 18:7-28

See also Procedure and decisions of the Chair; Subcommittee

Revenue Department, see Data—Storage**Robinson, Mr. Ken** (L—Ettobicoke-Lakeshore; Parliamentary

Secretary to Minister of Justice and Attorney General and

Minister of State for Social Development)

Access to information, 5:35

Banks and banking, 4:14-6, 19; 5:32; 13:22-5, 29; 14:9-10

Canadian Bar Association, 16:30-1; 17:11-2

Canadian Business Equipment Manufacturers Association, 3:12

Canadian Information Processing Society, 12:12-5, 18

Child abuse, 16:38

Computer services, 1:46-7; 7:29; 11:19; 15:24; 17:14

Computers, 3:12-5; 4:20; 7:29; 10:21; 15:25; 16:31, 35

Copyrights, 5:12, 17; 7:20; 11:13-6, 20; 13:26; 16:29

Criminal Code, 1:43; 2:37-8; 3:21; 5:10; 6:32; 7:28-9; 11:18; 12:20, 23; 16:30, 36

Criminal Code Bill (computer crime—C-667) (subject matter), 1:13-8, 31-2, 40-51; 2:4-6, 10-2, 20-38; 3:6-7, 11-2, 19-26, 29-31;

4:14-20; 5:5, 8-13, 16-8, 30-7; 6:4, 8, 17-32; 7:20-34; 9:28-35;

10:14, 16-26; 11:8-10, 13-22; 12:4-5, 12-25; 13:4, 7-10, 20-30;

14:9-15, 22-3; 15:4, 21-33; 16:28-40; 17:11-8, 23, 27-34

Data, 1:44; 2:20; 3:24-5; 4:16; 5:11; 6:23-5; 9:30, 34-5; 10:24; 11:8, 14-9; 13:20-1, 26; 14:10-3; 16:36; 17:12, 30

Data theft and/or destruction, 6:18-21, 28; 14:12-3, 22

Definition, 4:17; 15:21-3, 26-7; 16:23

Evidence, 17:15-6, 28-33

Evidence Act, 1982, 13:7-8; 16:34; 17:28-33

Government, 6:29

House of Commons, 2:33

Robinson, Mr. Ken—Cont.

Industry, 10:19; 12:17, 24

Intellectual/industrial property, 11:20-1

Investigation and enforcement, 1:45; 3:28; 5:9; 7:33; 12:19-21;

13:26-9; 14:10; 15:29; 16:37-8

Jurisdiction, 1:41-3; 3:19; 5:10, 23; 6:32; 7:20-1; 9:28-30, 33;

10:24-5; 13:20-1; 15:22-8, 31; 17:13

Law Reform Commission, 1:50

Legislation, 1:43-4; 4:19; 5:35-6; 9:29-30, 33; 15:30

Offences, 4:19-20; 6:24-5; 10:24-5; 12:22-3; 13:20-1; 15:25; 16:30, 36-7

Offenders, 3:20

Organization meeting, 1:7-13

Patents, 16:31

Points of order

Clerk, 1:44

Documents, 3:6

Ms., 15:33; 16:28

Meetings, 1:11

Order of reference, 1:8-9

Questioning of witnesses, 1:31-2, 40, 47; 2:4

Reports to Committee, Ms., 2:4; 18:30

Witnesses, 1:14-5, 31-2, 44; 3:31; 4:20; 9:28; 12:16; 15:31

Prevention/deterrence, 1:45; 2:24, 27-9; 3:19-20, 26; 4:15; 5:9; 9:32, 35; 10:20; 12:15-6, 23; 13:25-6; 14:14-5; 15:28-9; 16:39

Privacy, 5:30-2, 35; 14:9-12, 22; 17:12-3

Royal Canadian Mounted Police, 1:51

Security, 2:7, 23-5, 34-6; 3:15-9, 25, 30-1; 6:18-22, 28-31; 7:30-3; 10:17-9, 23-5; 12:16-22; 13:25; 15:26-7

Software, 10:22; 15:24-5; 16:38-9

Subcommittee, 1:17

M., 5:3

Surveys and studies, 1:40-1; 5:8, 30

Television, 6:26-7

United States, 5:34-5; 15:20-3, 26-31

Wiretapping and eavesdropping, 6:22-3

Rosen, Mr. P. (Researcher, Library of Parliament)

Organization meeting, 1:13

Rous, Mr. Collin C. (Cerberus Computer Security Inc., Toronto)

Criminal Code Bill (computer crime—C-667) (subject matter), 2:10-25, 28-9, 32-8

Royal Canadian Mounted Police

Draft legislation proposal, soliciting, 1:51

See also Organizations/individuals appearing and briefs submitted

Satellites, see Wiretapping and eavesdropping**Security**

Accidental incidents, prevention, 4:8; 7:7; 8:8

Computer systems, public access, 2:17-23, 26, 30; 7:32-3

Corporate responsibility, 8:7-11, 14-6; 9:8-9, 13-4, 17, 24, 31-2; 10:7; 12:8-12, 21; 15:26-7

Electronic data processing security officers, role, 12:5-6, 16-7

Employee screening, human rights legislation interfering, 2:8, 25; 10:24

Encryption, log-ons, data encryption standard (DES), etc., 3:15-8, 25; 6:9, 13-4; 7:10-1, 14, 18, 26; 9:12-3; 12:18-9, 23; 13:12

Encryption, theft

Locksmith program, 9:12

See also Data theft and/or destruction—Trojan

Fallibility, 7:14; 12:19; 13:28-9

False information, planting, 7:30-2

Government department guidelines, 10:10-1, 14, 25

IBM Corporation, 1972 study, 2:36

Insurance, 12:10-1; 13:17-9

Internal, employee education, 1:47; 12:6, 19-20; 13:25

Security—Cont.

- Internal/external, 2:23-4, 34; 3:17-8, 28-31; 7:17
- Legislation, international comparison, 10:18-9
- Licensing requirement, establishing, 7:32-3; 9:16
- Marketing of systems, effectiveness, etc., 3:16-9, 25, 30-1; 6:18-9; 8:21; 10:17-8
- National, current legislation, 6:30
- See also Official Secrets Act
- Physical/technological, 2:20-1; 3:25; 7:26; 12:6
- Project Mac, U.S. government project, fail-safe system, 2:13; 6:6-7
- Risk-analysis, 12:21-2
- Sensitive data, alternate storage, 2:37; 3:31
- "Sleeping bugs", 10:11, 23
- Standards, legislation, 9:24, 31-2; 12:8-10; 13:14-7; 15:20; 16:25
- Tempestization, screening process, costs, U.S. National Security Agency guidelines, etc., 6:18-22, 28-31
- United States military, "Tiger Teams", 7:14; 13:28
- See also Government; House of Commons; Mitel Corporation; Software—Licensing

Social insurance number

- Fraudulent use, 17:26-7
- See also Privacy

Software

- Definition, 16:12; 17:7
- Duplication, unauthorized, prevention, 9:11-3, 34; 10:11-2; 15:24-5
- Licensing contracts, security guidelines, definitions of terms, etc., 10:7-11, 22
- "Locksmith" program, see Security—Encryption
- "Machine-readable", defining, 10:8, 22; 16:8
- Protection *Ontario Lawyers' Weekly*, May 20/83 article, *Software Insecurities—Computer Programs and the PPSA*, 16:38-9
- Vendor distribution, limiting, 7:18-9
- See also Copyrights; Data theft and/or destruction—Microcomputer; Japan; Trade

Spitzer, Mr. Frank (Consultant, Toronto)

- Criminal Code Bill (computer crime—C-667) (subject matter), 7:12-9, 20-34

Stanford Research Institute International, see Surveys and studies—Parker, Mr. Donn**Subcommittee**

- Name, M. (Mr. Lachance), 1:8, agreed to, 4
- Reports to Committee, printing, special edition, 18:30, agreed to
- Reports to Committee, progress report date, 1:10, 17-8, 51
- Staff, 1:12
- M. (Mr. K. Robinson), agreed to, 5:3

Supreme Court, see Computer services—University of Alberta**Surveys and studies**

- Consumer and Corporate Affairs Department, Dr. John Palmer, 5:6-8, 17, 30
- Employee attitudes, John Carroll, University of Western Ontario, 2:8; 7:16
- Employee attitudes, U.S. Institute of Internal Auditors, Inc., 2:8
- Legislation, review, Professor R.G. Hammond, Alberta Institute of Technology, 1:25, 43-4, 50; 9:22-3
- Ontario Provincial Police, 1:22, 41; 2:16; 4:6
- Parker, Mr. Donn, Stanford Research Institute International, 1:21, 30, 40; 2:17, 21; 4:17; 10:5; 15:5, 13-4, 29
- See also Security—IBM Corporation; White collar crime—Pitney Bowes Corporation

Sweden, Data Act, 1973, 5:28-9; 7:21; 9:25; 15:31**Symposium on Computer Crime and Privacy**, Brookings Institution, November 1982, 1:28-30**"System Hacking"**, see Computer services**TAP**, see Computer services—Publications**Technology**, see Computers**Telecommunications**, offences, inclusion, 16:13-4; 17:6**Telephones**, see Bell Canada; Data theft and/or destruction; Wiretapping and eavesdropping**Television**

- Electro-magnetic radiation (EMR) monitoring, ratings and tax calculations, 6:7-8, 26-8
- Pay TV decoding equipment, legality, 6:11, 16-7, 27-8; 8:12
- Pay TV decoding, Northern Alberta Institute of Technology contest, 9:13

Telidon System, potential abuse, 2:30**Tempestization**, see Data theft and/or destruction—Remote access; Security**Tollefson, Mr. E.A.** (Co-ordinator, Criminal Code Review, Justice Department)
Criminal Code Bill (computer crime—C-667) (subject matter), 17:17-33**Trade**, software, international anti-dumping regulations, applying, 10:12-3**Trade secrets law**, see Data—Protection**Trademarks**

- Legislation, revision, 11:21
- See also Data—Protection

Trespass, see Offences—Defining**Trojan horse scheme**, see Data theft and/or destruction**Uniform Law Conference**, see Evidence Act, 1982**United States**

- House of Representatives Subcommittee of the Judiciary Committee on Constitutional and Civil Rights, Parker and Nycum testimony, 15:20; 15A:1-6
- Legislation, 1:28-9; 3:23-4; 9:4, 10; 12:8, 22; 15:12, 15, 21-3, 26-32
- Offenders, restitution, legislation, 1:27
- Privacy legislation, 5:20-2, 34-5
- Reporting requirements, 1:23, 27; 4:22; 5:28; 15:15
- Right to Financial Privacy Act, 1978, 5:23
- See also Patents; Security—Project Mac—Tempestization; Surveys and studies—Employee attitudes; White collar crime

Universities

- Computing ethics courses, 12:16; 13:15; 14:18
- Violations, 5:25-6; 7:9-10, 13

University of Alberta, see Computer services**University of Toronto**, computer facilities, 7:14**University of Waterloo**, see Computer services—"System hacking"**University of Western Ontario**, see Surveys and studies—Employee attitudes**Video games**, see Copyrights

Ward, Mr. Peter (Peat, Marwick and Partners, Toronto)
Criminal Code Bill (computer crime—C-667) (subject matter),
4:4-26

Watkins, Peter, *see* Offences

West Germany, banking, privacy legislation, 5:24, 32

White collar crime

Causes, prosecution, deterrence, etc., 8:4-6, 22
Pitney Bowes Corporation study, 8:5
United States 1967 Commission on Law Enforcement and the
Administration of Justice, 8:4-5

Wiretapping and eavesdropping

Laser beams, 6:22-3
Microwave interception, etc., 6:10-2, 17
Satellite beam interception, 6:11-2

Woodhead, Mrs. Sally (Chairman of Special Interest Group on
Computer Security, Canadian Information Processing Society)
Criminal Code Bill (computer crime—C-667) (subject matter),
12:4-24



If undelivered, return COVER ONLY to:
 Canadian Government Printing Office,
 Supply and Services Canada,
 45 Sacré-Coeur Boulevard,
 Hull, Québec, Canada, K1A 0S7

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à:
 Imprimerie du gouvernement canadien,
 Approvisionnements et Services Canada,
 45, boulevard Sacré-Coeur,
 Hull, Québec, Canada, K1A 0S7

BINDING SECT. SEP 20 1984

